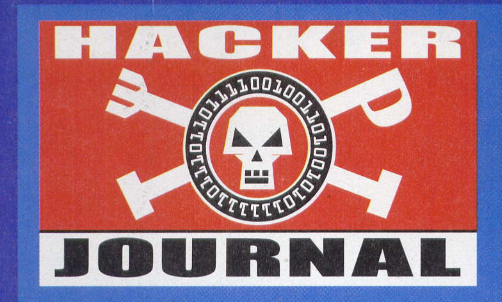

N.8
bimensual
año 2 · 2004
HACKER
JOURNAL
www.hacker-journal.com
MÁS QUE UNA ESPERANZA
HOPE 5
2€
SIN PUBLICIDAD
SÓLO INFORMACIÓN Y ARTÍCULOS
8 414090 031417 00008
4ever
WANTED
DEAD OR ALIVE
Windows XP secreto
TRUCOS
PARA LA RED
Y CREAR ARCHIVOS
COMPRIMIDOS
EL PENTÁGONO
ESPIADO
POR SATÉLITE
CRÓNICA
DE UN ATAQUE
al servidor
de la escuela
MARAVILLAS DE JAVASCRIPT



Año 2 - N. 8 - 2004

Director Responsable:
Luca Sprea

Los chicos de la redacción europea:
Federico Cociancich, Amadeu Brugués,

Infoambiente, Gualtiero Tronconi, Eduardo Bracaglia, Gregorio Peron, Contents by MDR

Colaboradores: Bismark, Fabio Benedetti, Guillermo Cancelli, Gaia, Nicolás A., Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia,3dO, Mònica Batalla, Anna Riera

Maquetación: Estudi Digital, S.L.

Diseño gráfico: Dopla Graphic S.r.l. info@dopla.com

Redacción
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printed in Italy

Difusión: Paul-Luc PEREZ

Distribución
Coedis, S.L. - Avda. de Barcelona 225
08750 Molins de Rei (Barcelona)

Publicación bimensual registrada el 14/2/03 con el número MI2003C/001404

hack·er (hãk'ər)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios que prefieren aprender solamente lo mínimo necesario."

MOTIVOS PARA LA ESPERANZA

Recientemente se celebró la conferencia HOPE 5, de la que damos cumplida información en las páginas ocho a once. Es en actos de este tipo donde se percibe la fuerza imparable de los colectivos de personas concienciadas, decididas a luchar por sus derechos y por el más simple de ellos: el derecho a disfrutar de la vida, libremente y sin aranceles abusivos.

Los peligros que acechan al usuario medio de informática, y por extensión a cualquier ciudadano que tenga datos circulando por la Red, son muchos y de distinto tipo. Desde los estafadores de poca monta hasta organizaciones de altos vuelos, pasando por gobiernos con secretos y sin escrúpulos, o fabricantes ventajistas dispuestos a sacar provecho de la situación. No hay que olvidar, por supuesto, a los bromistas sin criterio que hacen daño, entre otros, a quienes nos sentimos orgullosos de ser, o de intentar llegar a ser, hackers. Nuestra visión de la justicia en el mundo cibernético también se ve comprometida, y por ello queremos, desde estas páginas, dar apoyo a todas las iniciativas para la defensa del ciudadano, del usuario.

A menudo tendemos a creer que las grandes iniciativas sólo se producen muy lejos de aquí. Nada más lejos de la realidad: desde nuestros limitados recursos, podemos hacer muchas cosas para mejorar la situación y convertirnos en garantes de la libertad y la alegría de vivir. En Hacker Journal todos, redactores y lectores, podemos intercambiar puntos de vista, conocimientos y tolerancia para sembrar la semilla. Otras iniciativas están en marcha: echad un vistazo a la noticia sobre la campaña contra el canon en los CDs y DVDs. De tan sencilla, parece casi imposible. Y sin embargo, se mueve. Buscando, buscando, seguro que entre todos encontramos mil y un motivos para luchar, para ser felices con nuestro PC y con nuestra privacidad. Nos va la calidad de vida en ello.

redaccion@hacker-journal.com

UNA REVISTA PARA TODOS


NEWBIE

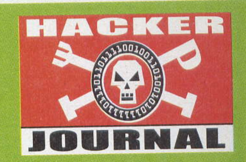

MID HACKING


HARD HACKING

El mundo hacker se compone de algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal está marcado con una clave para cada nivel: NEWBIE (para quien comienza), MIDHACKING (para quien ya está dentro) y HARDHACKING (para quien no existen los secretos).

SUMARIO

Número 8 - Septiembre - Octubre 2004

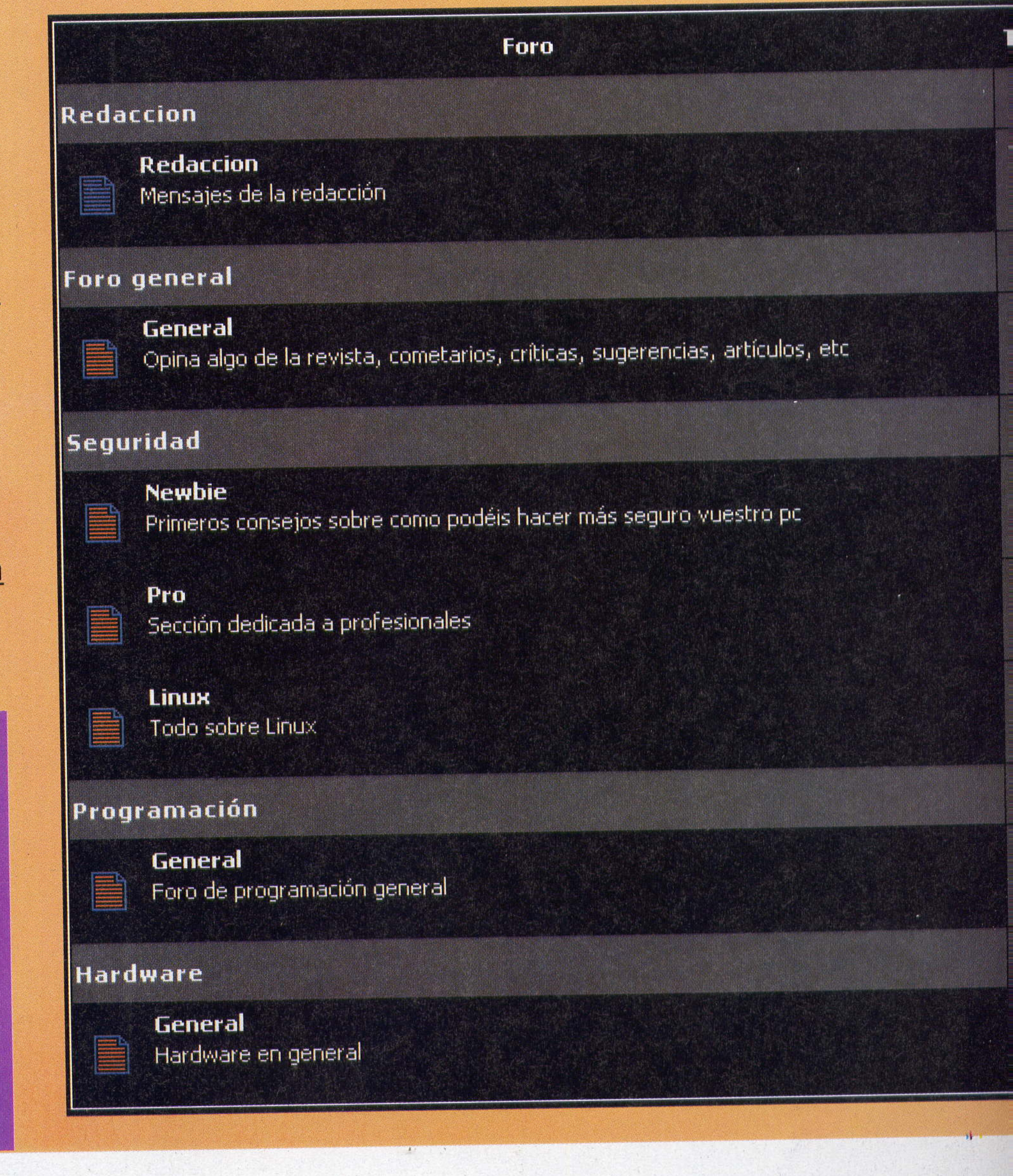


SITIO WEB

¡Hemos habilitado nuevos foros! Debido a las peticiones de los lectores, se han puesto en marcha dos nuevos foros, uno dedicado a la Programación y otro al Hardware. Próximamente iremos creando categorías en su interior, para adecuarlos a las contribuciones de los visitantes.

Escribidnos a redaccion@hacker-journal.com

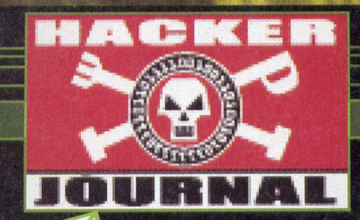
Visita nuestro sitio web: **www.hacker-journal.com**



¡SECRET ZONE RELOADED!

Y más problemas técnicos. En esta ocasión, ha sido un problema de actualización de contraseñas. Es la hora de redoblar esfuerzos para que todo funcione como es debido. De momento, podréis acceder a los números 1 y 2 de nuestra revista, y pronto incluiremos más números. Manteneros en contacto. Con algunos navegadores, puede ser necesario insertar dos veces los mismos códigos. No os detengáis al primer intento

user: 8secret0
password: cel4dobl3



mailto:
redaccion@hacker-journal.com



PROBLEMAS CON SECRET ZONE

Hola. Era para decirles que al introducir los codigos de la ultima revista en la secret zone, no me deja entrar. ¿Saben si estos son los codigos para entrar? si no se soluciona, ¿podrian mandarme los dos archivos a mi correo ? Gracias.

Alfredo

Efectivamente, los códigos eran los correctos... pero no se realizó el cambio cuando era el momento y la secret zone ha seguido funcionando durante bastante tiempo con los códigos del número 6. Sólo faltó la llegada del verano y las vacaciones para que todo se complicara innecesariamente y no se resolviera como es debido. Pedimos disculpas a todos nuestros lectores por este problema. A la vuelta de vacaciones redoblaremos esfuerzos para que acaben los problemas con nuestra área 51 particular...

NÚMEROS ATRASADOS

¡Hola! Soy Jesús. Me gustaría saber cómo se pueden conseguir los números atrasados del 7 hacia atrás de Hacker Journal. También me es imposible registrarme en su Web, si son tan amables de informarme .
¡Un saludo, gracias!

Jesús

Los números atrasados pueden conseguirse en la secret zone de nuestro sitio web, www.hacker-journal.com, para cuyo acceso tienes que utilizar los códigos que indicamos en la página 3. Respecto a cómo registrarte en el sitio web, cuando accedas a la página principal, fíjate en la parte final de la columna de la izquierda: bajo



"¿Quién está online?" puedes hacer clic en el enlace "aquí" y pasarás a la ventana de registro. ¡Te esperamos!

ELIMINAR DATOS

¡Hola!
Después de leer vuestro ultimo numero, me hice algunas preguntas sobre el tema de la destrucción de datos segura. Deciais que para que los datos de un ordenador no se pudieran recuperar se tendría que formatear 10 veces y machacar a pedacitos los chips. Pues aquí va la pregunta: Si se construyera un programa que cambiase aleatoriamente todas las letras y numeros del codigo fuente por otros, ¿se podría recuperar el archivo?
P.D. Electro, (el que os criticó en el ultimo numero) si lees esto me gustaria decirte que esta revista es la mejor que he encontrado por precio, calidad, contenido....

SYPHER

El problema principal sigue siendo el mismo: a pesar de borrar y sobreescribir una posición en el disco, sigue quedando una sombra magnética en dicha posición que permite, con el material adecuado, llegar a recuperar la información original. Por supuesto que utilizar un programa que reescriba los datos aleatoriamente es una buena solución, pero no nos libra del trabajo igualmente fundamental: escribir todas las veces necesarias sobre las posiciones primitivas. Cuidado, que no sirve escribir sólo el archivo de nuevo, porque es posible que la versión primitiva se marque simplemente como espacio disponible y el archivo cambiado vaya a parar a otra posición del disco. Es básico: 1.- Escribir en las mismas posiciones originales del disco, y 2.- escribir nuevos contenidos tantas veces como sea posible. Si sobreescribes el número suficiente de veces, la verdad es que poco importa que escribas ceros o bien caracteres aleatorios.

ALLENDE LOS MARES

Hola amigos de Hacker Journal, gracias por su respuesta, felizmente los numeros de hacker journal acá ya llegaron hasta la cinco y me los compre todos, la mala noticia es que la importadora de España no va enviar mas ejemplares acá a Perú, de esto me enteré cuando me compré en la misma importadora las revistas Riguse en Perú. Acá la revista está recién siendo conocida ya que no es muy apoyada. Pero la importacia del contenido de esta revista es valioso para cualquier usuario de una PC.
Me he contactado con un compañero español que me puede mandar las revistas pero es muy caro 60 dolares por ejemplar.
Puedo pagar hasta 20 dolares máximo por ejemplar. Espero que implementen esa modalidad

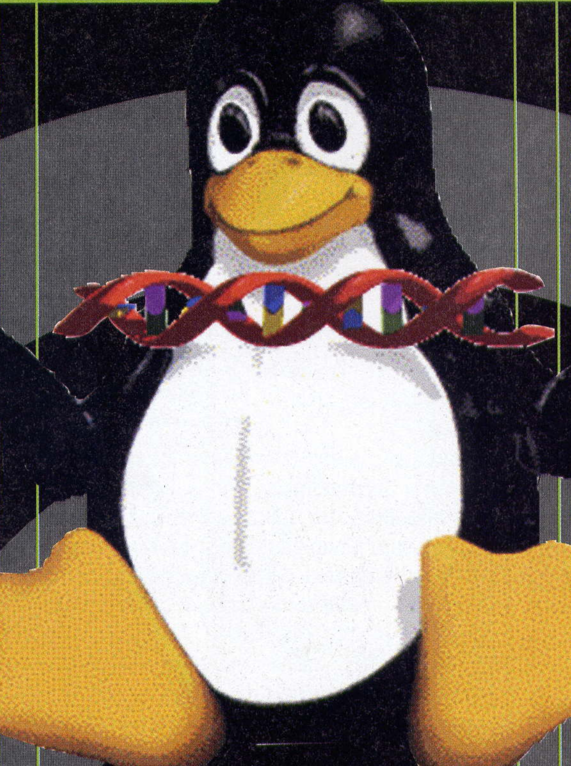
Atentamente

Miguel Castilla

¡Gracias Miguel por tu interés en Hacker Journal! Debido a algunos problemas con la distribución también en España, cambiamos recientemente de distribuidora. Es probable que la nueva distribuidora se preocupe de dar continuidad a la distribución en Perú, aunque lógicamente la anterior deje de hacerlo.
El método de ponerte de acuerdo con alguien para que te mande las revistas es perfecto. Tal vez, para reducir costes, te salga a cuenta recibir varios ejemplares juntos en lugar de recibirlos uno a uno. Es algo que tienes que hablar con tu contacto en España. Por nuestra parte, sólo podemos agradecerte el interés que muestras por nuestra vuestra revista.

¿LINUX?

Buenas,
he comprado vuestra revista desde el primer número y la verdad, me parece bastante entretenida y me gusta XD. Pero hecho muuuuuuuuchoooooo en falta algo sobre linux. Por ejemplo en este último numero el artículo de Microsoft me parece expléndido, pero veo contradictorio que después de decir: "Pues no señores. No podemos continuar comprando PCs que tengan instalado un único sistema operativo sin tener opcion a decidir cómo queremos que funcione nuestro ordenador" (cito textualmente). y luego en el apartado de "HACK TOOLS" sólo hableis de herramientas para Windows. Vale que mucha gente nueva usa Windows, y asi os asegurais mercado (con perdón) y ademas que la gente os entienda. Pero creo que deberiais poner informacion sobre linux, distribuciones, cuales son faciles y dificiles, y asi interesar un poco a la juventud actual ke solo saben ver las ventanitas y el raton, que no saben ke es una shell, ni un telnet... Al mismo tiempo si poneis HACK TOOLS de windows, no costaba nada poner alguna de linux y algun artikulo donde salga linux y que no parezca un SO de elite, pork no lo es, es un SO muy completo, de los que estan mejor comentados y dificil al principio, eso si, pero despues va perfecto.



En resumen, opino que la revista esta muy bien pero ke esta muy enfocada a Güindoze y eso no me parece eticamente correcto ya que la etika "hacker" esta en contra de la privatizacion de codigo y de informacion, o hemos olvidado pork empezó todo?
Eso si, es una gran revista, es el fallo ke le encuentro ke solo hay windows xD
mucho gusto de contactar con ustedes y sigan mejorando, por cierto, cuando lean el e-mail porfavor respondame aunk sea diciendo: lo hemos leido xD
adios y mucho gusto

PD: si necesitais a alguien k eescriba algo decirlo a kambio solo pedire vuestra revista de manera gratuita xD gracias..

HaK hakmaster

No te preocupes, en cuanto nos salgan las ventas por las orejas empezaremos a mandar ejemplares a todos los interesados :-) Esperamos que comprendas que no estamos para grandes regalos. Precisamente para llegar al máximo de gente es por lo que Windows ocupa un espacio destacado en el uso de herramientas y utilidades. Naturalmente que estamos de acuerdo en que el uso del shell abre unas posibilidades enormes, pero no es menos cierto que su uso requiere una formación suplementaria que no todo el mundo quiere o puede permitirse (hay gente con poco tiempo disponible para investigar). Sin embargo, en cada número incluimos pequeñas dosis de Linux, hablamos de instalar diferentes distribuciones, de compabilizar su uso con Windows... No queremos exigir a nuestros lectores un dominio completo de este magnífico sistema operativo para que puedan leernos. Pero sí nos gustaría sabernos partícipes del movimiento imparable que, lentamente pero de forma segura, va llevando cada vez a una plataforma más amplia de usuarios hacia las distribuciones de Linux.
También estamos completamente de acuerdo en que Linux no es un sistema operativo de élite. Es más, con cada nueva distribución que aparece se facilita progresivamente la instalación. Muchas distribuciones exigen menos tiempo y conocimientos para su correcta instalación que las últimas versiones de Windows. Y las interfaces gráficas de Linux no tienen nada que envidiar (antes al contrario) a los sistemas más extendidos. Pero ciñámonos a lo que hay: millones de usuarios de Windows que desconocen totalmente el uso de Linux, que han adquirido y se han habituado a una serie de aplicaciones, y para quienes descubrir un nuevo sistema operativo, y una nueva gama de aplicaciones, no resulta fácil. Cuando compras un PC para jugar en casa, bastante tienes con conseguir que se conecte a Internet. Hasta que un porcentaje suficiente de sus vecinos no tenga instalado Linux y pueda echarle una mano en las miles de dudas que surgen con sólo encender el PC, es difícil que ese usuario queme las naves y se decida por el cambio que puede cambiar su vida.

HOT!

➲ MESSENGER, HASTA EN MERCURIO

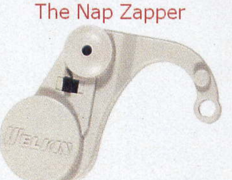
No, no se trata del popular software de chat. Se trata de una nueva nave espacial que se dirige al planeta Mercurio. El 2 de agosto empezó su viaje, que se prolongará durante unos siete años antes de llegar al planeta más caliente del sistema solar.
El interés de estudiar Mercurio estriba en que comparte su naturaleza terrestre con Venus, la Tierra y Marte, de manera que su estudio puede aportar datos para comprender cómo se formaron estos planetas derivados de la nebulosa solar primigenia.
En cuanto a su temperatura, hay que indicar que es más bien un planeta de contrastes. Debido a que su atmósfera es muy tenue, no distribuye el calor por el planeta, de modo que en las zonas expuestas a la insolación la temperatura alcanza los 450ºC, mientras que en las zonas a la sombra se mantiene a -180ºC.
El Messenger lleva siete instrumentos científicos para conseguir imágenes de todo el planeta, así como información sobre la composición de la corteza, el núcleo y los materiales polares, su historia geológica, y la naturaleza de su atmósfera y su activa magnetósfera.

➲ LAS PYMES ESPAÑOLAS NO PASAN EL EXAMEN DE SEGURIDAD EN RED

Una encuesta realizada por la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC) asegura que la mitad de las pymes españolas no cumplen los mínimos indispensables de seguridad en la Red
ASIMELEC encuestó a más de mil empresas de toda la geografía española para constatar el nivel de seguridad en Red que poseen las pymes en España y hacer un seguimiento de dichas empresas sobre el cumplimiento de la norma internacional ISO/IEC 17799:2000 que constituye el código de buenas prácticas de la gestión de la Seguridad de la Información.
El 12 % de las empresas encuestadas no tiene una mínima defensa antivirus, el 57% de las pymes no cuentan con otro tipo de herramienta de defensa en red, y menos del 4% realiza inspecciones regulares de contenidos.

➲ DISPOSITIVO ANTISUEÑO AL VOLANTE

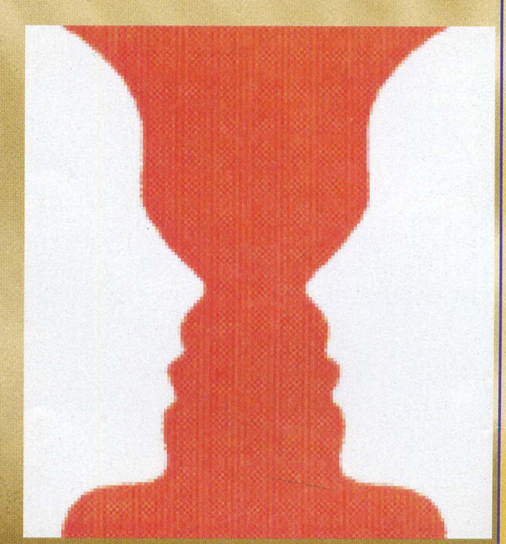
Los conductores españoles han comenzado a comprobar la eficacia de un aparato contra la somnolencia que emite pitidos de aviso cuando la cabeza se inclina a causa del sueño.
El dispositivo, de reducidas dimensiones, va colgado a la parte trasera de la oreja y se activa al producirse las características cabezadas.



Parece ser que se trata de un dispositivo muy eficaz y de peso muy liviano. Ha empezado a ser distribuido por algunos médicos y próximamente será posible adquirirlo en las farmacias.
El aparato consta de un sensor electrónico de posición y sirve también para trabajos que requieran atención constante, particularmente en horarios nocturnos, como el manejo de maquinaria pesada y de mercancías peligrosas o actividades de vigilancia y seguridad. También puede ser útil para personas con trastornos del sueño como la narcolepsia, que consiste en una excesiva somnolencia diurna y la alteración del sueño nocturno.
En 2003, hubo ciento doce accidentes mortales en las carreteras españolas que se atribuyeron a la somnolencia, un 33,3 por ciento más que el año anterior, según datos de la Dirección General de Tráfico. Estos representaron el 3,3 por ciento de todos los siniestros con fallecidos.
El aparato, llamado Nap Zapper (en inglés "anulador de la siesta", ya se comercializa en Estados Unidos y su precio ronda los doce euros.

➲ PERSONALIDADES DIFERENTES EN INTERNET

Según un estudio diseñado por investigadores de la Universidad de Salamanca existen cuatro perfiles diferentes de usuarios de Internet. Según los resultados del estudio "Perfiles de Personalidad Diferenciales de los Usuarios de Internet", elaborado por la Universidad de Salamanca, que tiene entre sus objetivos la investigación para la intervención en casos de adicción, existen cuatro tipo de internautas: Profesionales, Aficionados, Perturbadores y Adictos.
El estudio descriptivo permite atribuir ciertos patrones de conducta y rasgos específicos a los internautas.
Los profesionales son quienes dedican largos periodos de trabajo al uso del ordenador y de Internet para conseguir información, crear contenidos o programas, y si bien esto puede crear adicción.
Los aficionados, interesados en la Red por sus contenidos y para lograr propósitos, hacer intercambios o socializar, pero todo en un marco de normalidad.
Los perturbadores son un grupo heterogéneo



de sujetos que por motivos distintos emplean Internet para perjudicar, molestar, aprovecharse y causar daños y problemas a otros.
Los adictos dependen y piensan demasiado en Internet, que interfiere en el desarrollo normal de su vida, actividades y obligaciones.

DEMANDA CONTRA EL CANON DE CD Y DVD

Los detractores del canon sobre los CD y DVD que estén dispuestos a batallar contra una medida que consideran injusta e inconstitucional pueden interponer una demanda que circula por Internet. El objetivo de sus promotores es llevar el problema ante el Tribunal Constitucional (TC) para que se pronuncie sobre la inconstitucionalidad del artículo de la Ley de propiedad intelectual sobre el que se basó un acuerdo entre las entidades de gestión de los derechos de autor y los fabricantes de soportes informáticos para compensar a los músicos por la copia privada. De momento, 25 ciudadanos han presentado otras tantas demandas en los juzgados de sus respectivas localidades. Reclaman a las tiendas donde compraron los CD ROM vírgenes que les devuelvan el importe del canon por ser inconstitucional.
La demanda, de 75 folios, va acompañada de la factura en la que consta el desglose del canon. Los demandantes pueden incluso descargarse la llamada nota para la vista, el documento que deben presentar ante el tribunal cuando se celebre el juicio. Como es una pequeña cantidad (entre 0,17 y 0,70 euros según sean para datos o audio), no hay costas judiciales ni son necesarios abogados ni procuradores. "El máximo perjuicio que pueden sufrir los denunciantes es perder una mañana en los juzgados", dicen sus promotores.
La demanda defiende que se ha impuesto un canon al soporte de registro de la civilización: los soportes digitales de hoy equivalen al papel de hace 30 años.

ITUNES PARA LINUX

Codeweavers, un desarrollador de software especializado en software que permite correr progrmas de Windows sobre Linux, dispone de una nueva versión de su software que ofrece soporte a iTunes.
La compañía ha dicho que Crossover Office 3.1 añade soporte para el reproductor de audio y la tienda en internet, ha informado C|Net.
La versión actual se encuentra aun en una fase temprana (preview) y solo está disponible para los usuarios de CrossOver. La versión final se espera a lo largo del final de este año.
Apple no ha creado una versión para Linux de iTunes.
Desde su lanzamiento en 2002, CrossOver Office ha impactado en el crecimiento y uso práctico del sistema operativo Linux entre los usuarios de PC. CrossOver Office habilita muchas aplicaciones de primera línea de Windows incluyendo Microsoft Office, Internet Explorer, Visio Quicken, Macromedia Dreamweaver y Flash, y Apple QuickTime haciendo que operen de forma nativa bajo Linux sin emuladores secundarios.
Más información: www.codeweavers.com.

HOT!!

CIERRA LA REVISTA ELECTRÓNICA EN.RED.ANDO

La revista electrónica En. Red. Ando, dedicada a difundir la cultura digital y a la asesoría de empresas e instituciones en comunicación electrónica y gestión de conocimiento, ha cerrado tras ocho años de presencia en Internet.
En. Red. Ando, aparte de publicar artículos sobre cultura digital en su revista en Internet, organizaba masters y acatuaba como consultora de empresas. Su web (www.enredando.com) ha quedado fuera de servicio, aunque el director de la revista ha anunciado que la intención es que los artículos publicados puedan estar pronto disponibles.

ACTUALIZACIÓN CRÍTICA PARA INTERNET EXPLORER

Microsoft ha roto su costumbre de publicar cada segundo martes de mes boletines con soluciones para fallos de sus productos, al anunciar el pasado viernes una actualización de seguridad "crítica" para su navegador 'Internet Explorer'.
Así, en lugar de esperar al 10 de agosto, la compañía recomendó la instalación "inmediata" de la actualización MS04-025, que corrige tres vulnerabilidades públicas descubiertas recientemente, y que permiten la "ejecución remota de código y pueden ser empleadas por virus o intrusos", según apuntó la consultora independiente de seguridad Hispasec.
Microsoft reiteró a los usuarios la necesidad de actualizar sus equipos informáticos para prevenir ataques de virus, pidiéndoles que instalen "lo antes posible" la actualización, a la que concedió la clasificación más alta de importancia, es decir, 'crítica'.
Hispasec explicó que el primero de los problemas anunciados se trata de una vulnerabilidad de ejecución remota de código en 'Internet Explorer' debida al modo en que se tratan los métodos de exploración.
Un intruso podría aprovechar esta vulnerabilidad mediante la construcción de una página web o 'e-mail' con html malicioso, lo que permitiría la ejecución remota de código cuando el usuario visitara el sitio web.


IG BROTHER IS
VATCHING YOU

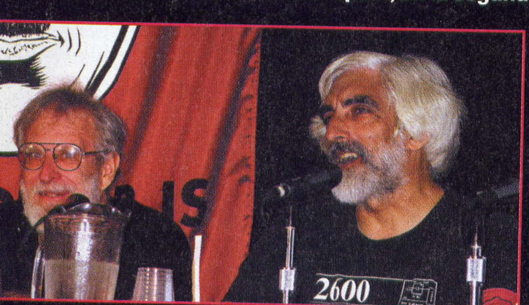
HOPE 5 ¡más que una esperanza!

Hackers on Planet Earth ha llegado a su quinta edición. Organizada por la histórica revista americana 2600, de periodicidad bianual, HOPE es el punto de referencia sociopolítico para los hackers americanos.

A diferencia de DefCon, HOPE está claramente orientada a los problemas sociales de los hackers y está comprometida políticamente con la libertad de expresión y el soporte a la comunidad americana y extranjera, donde los derechos se conculcan más fácilmente. De hecho, la ambientación de la conferencia es muy particular. Simbolismos de fuerte contenido político (de derechas y de izquierdas) cuelgan de las paredes y un enorme póster del gran hermano (con un curioso parecido con Hitler) recuerda a la audiencia que les está observando. Todo ello completado con los brazaletes negros que había que llevar en el brazo (aunque muchos hackers se lo colocaron en el cuello, en la pierna, en la cintura y en otros sitios demasiado difíciles de contar).

Ex hacker, ahora star

Durante tres días han desfilado por dos atriles de la convención nombres importantes de la historia presente y pasada de la informática. El primero de todos el Capitán Crunch, un icono del phreacking de los años 70, que participó en diversas conferencias en diferentes papeles, la primera como cabecilla de su propia campaña en contra del spam, en la segunda, junto con un viejo amigo suyo, Cheshire Catalyst, para contar las impresiones y las anécdotas de los viejos tiempos, e incluso junto a Wozniak como héroe de Steve y posteriormente como empleado número 13 de Apple y finalmente con Kevin Mitnick cuando se habló de Social Engineering. En realidad, toda la conferencia tiene un hilo lógico que cohesiona y une a todas estas personas en una única y larga historia que se despliega durante las tres jornadas.



↑ *Capitán Crunch y Cheshire Catalyst. Han combinado en todos los colores viajando por medio mundo. Iban indicando los problemas a las compañías telefónicas que se maravillaban de su habilidad. Algunos no han sabido nunca que ellos no eran empleados...*

La situación china

Las sesiones se sucedieron en las tribunas tratando los argumentos más dispares, pero despertó una especial atención un seminario titulado "Cómo funciona la Gran Muralla china", referido, no sin cierto embarazo y desagrado, al uso de las tecnologías más avanzadas de Cisco para tener bajo control y censurar las comunicaciones del pueblo chino. (Cisco no confirma ni desmiente el hecho de proporcionar aparatos y tecnología, pero confirma que se han desarrollado versiones de firmware con características particulares para China). Existe de hecho una larga lista de IP prohibidas para el pueblo chino y otra larga lista de palabras prohibidas por los motores de búsqueda. Es interesante ver cómo los 18 Gigabits de la ▷

...toda la conferencia tiene un hilo lógico que cohesiona y une a todas estas personas en una única y larga historia...

ENTREVISTA A MR.2600

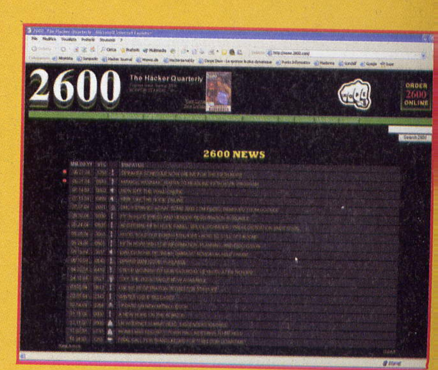
2600 es la revista histórica de los hackers americanos (¡y extranjeros!) y actualmente es una referencia para el sector. Hemos hecho dos preguntas a Emmanuel Goldstein, el editor de 2600:

HJ - ¿Cuánta gente participa en esta HOPE?

2600 - Más de dos mil personas han pagado 50 dólares por los tres días, un resultado verdaderamente interesante.

HJ – ¿Sigue teniendo sentido, con Internet, organizar estas manifestaciones?

2600 – Sí, es muy importante el contacto físico y verse en persona ayuda. ¡Especialmente ahora, cuando nuestra libertad está siendo atacada como nunca anteriormente!



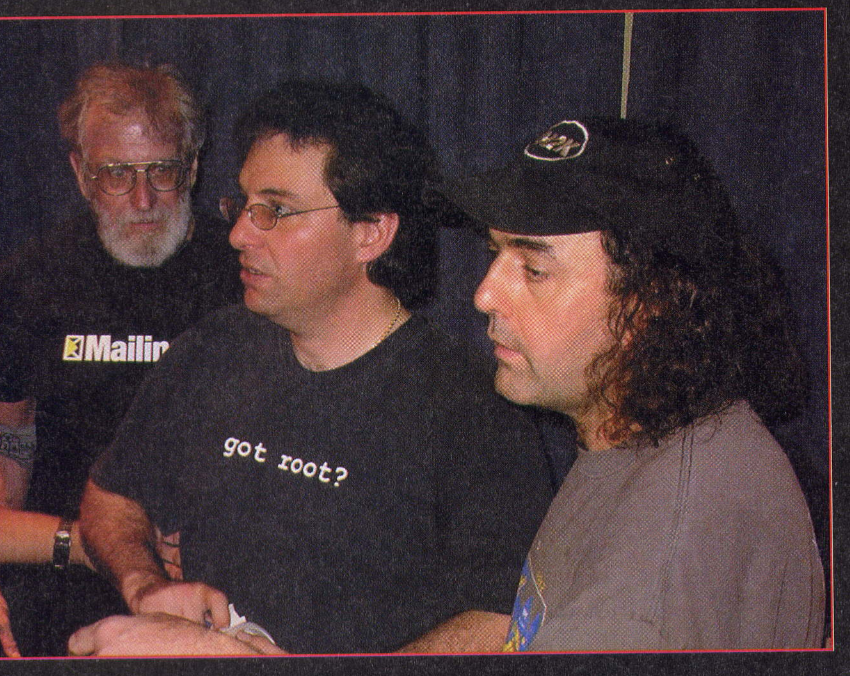
conectividad china pasan todos por el mismo router y cómo éste se ocupa de bloquear las conexiones de y hacia los IP prohibidos. También es interesante cómo al transferir cualquier paquete que contenga la palabra GET y un término prohibido, un dispositivo dos hops después del primer router pase a bloquear la conexión e inserte el IP en una lista de castigados durante unos 20 minutos.
Otro efecto interesante, también gestionado desde el tercer hop en el interior de la red china, es el DNS poisoning. Mediante esta técnica, al preguntar por el IP de un servidor cuyo nombre o IP está en la lista negra se obtienen dos respuestas distintas: una inmediata y errónea procedente del aparato gubernamental, y la segunda, que llega más tarde, del DNS real. Esto será un gran problema si Verisign quiere agregar un root DNS dentro de China, porque todas las peticiones para los DNS en la lista negra efectuadas incluso desde fuera de China darán resultados erróneos...



↑ *Count Zero presenta el nuevo curso de CDC fuertemente inspirado en el ACTIVism, que pide a todos los hackers del mundo que colaboren activamente en la defensa y la conquista de los derechos civiles en todo el mundo. ¡En Internet la situación de China es verdaderamente dramática!*

El cóndor

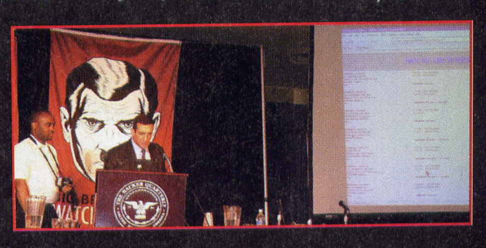
Pero todo el mundo durante el primer día esperaba al invitado de honor: ¡Kevin Mitnick! Kevin no había podido estar presente en las dos conferencias anteriores porque estaba aún en la cárcel en el 2000 y bajo vigilancia en el 2002 y por ello su presencia en la HOPE ha sido una manera de celebrar la libertad recuperada (y la aparición del nuevo libro titulado The Art of Intrusion).
Kevin recorrió en casi dos horas toda su historia, desde el principio hasta su reciente excarcelación. El público lo escuchaba en silencio rumoreando cuando Kevin recreaba los momentos más dolorosos de su experiencia, encerrado durante ocho meses en aislamiento total: 23 horas y media en una celda, solo, y media hora de paseo en un espacio también reducido, con esposas hasta para ir de la celda a la ducha.



↑ *Capitan Crunch - Kevin Mitnick - Emmanuel Goldstein: un terceto formidable, que representa la vieja y la nueva guardia de los hackers, bajo la protección de los medios.*

El segundo día

El segundo día de la conferencia la atención se centró en Steve Wozniak (the Woz). Steve explicó al auditorio sus experiencias juveniles como Hacker y como ingeniero; Woz ha sido siempre un apasionado de las bromas y explicó cómo había sido posible combinar su pasión por la electrónica con la realización de pequeños sistemas para interferir la TV y obligar al desafortunado de turno a jugar el desagradable papel de antena humana:



"[activo la interferencia] ya no a la izquierda [desactivo] ahora se ve [el tipo se mueve, activo] no, ahora no se ve... prueba con la punta del pie [desactivo] se queda en esta posición porque ahora funciona [en cuanto la víctima se mueve activo y así sucesivamente]".

Pero todo el mundo esperaba la historia y el principio del Apple I y II. Atormentado por la posibilidad de seguir trabajando con HP, Woz había intentado producir el Apple I para la propia



HP que lo había definido como "unmarketable" [imposible de vender] y le había entregado una liberatoria para poderlo comercializar por su propia cuenta. Convencido por Steve Jobs (que no había tenido éxito al recorrer al apoyo de parientes y amigos para convencer a Woz para que dejara HP y pasara a fundar Apple) finalmente cedió, seducido por la asignación de 25.000 dólares que una empresa local había destinado para la compra de 50 equipos Apple I.

Woz nunca se ha destacado por su amor al dinero, pero tenía una familia qu emantener y ahora encontraba la seguridad que andaba buscando para ser libre de seguir desarrollando ordenadores. Todos los proyectos del Apple I tuvieron una importante impronta del Homebrew Computer Club con cuyos socios había compartido todos los detalles de la plataforma de Hardware y Software del Apple I y posteriormente también de la del Apple II. Respecto al Apple II, Woz había intentado vender los proyectos a Commodore y a Altair pero ambos los rechazaron, dejándole fuera del mercado... Entretanto, en 3 KB Woz había desarrollado un Basic (gran parte del código fuente ha sido publicado en el Dr. Dobbs Journal) e insertó dentro del Apple II el sistema para la visualización a 8 colores y los gráficos de baja y alta resolución.

Finalmente, Woz dejó Apple con algunos millones de dólares: 28 menos algunos gastos para campañas de filantropía, unos 10 millones, y los negocios iban mal (no hay ironía en esto, pues otros habían ganado millardos de dólares...) pero sigue apoyando la arquitectura abierta, sabiendo que la verdadera riqueza está en el interior de su cabeza. Ahora Woz lanza una nueva empresa, Weels of Zeus, que implementa WiFi y redes celulares para la localización de personas y aparatos.



↑ *Steve Wozniak como siempre por la plataforma abierta: Steve Jobs decía que bastaban dos slots pero él quiso ocho en el Apple II.*

Mucho más preocupante, sin embargo, fue la intervención de Steve Rambadam. Steve es un investigador privado electrónico y mostró al público lo fácil que resulta obtener la información considerada privada y reservada. En una veloz sesión online, se ocupó de mostrar toda la historia de una pobre víctima que se prestó voluntaria al análisis, descubriendo incluso una posible estafa que podía incriminarle sin saberlo. El nombre mismo de la conferencia era inquietante: "La privacidad ya no es lo que era".

Es importante destacar que las leyes de otros países son mucho más robustas y restrictivas en cuanto a la privacidad, y por lo tanto un escenario de Gran Hermano como el que se da actualmente en los Estados Unidos es mucho más difícil de conseguir...

El último día

Fue el día de Jello Biafra, un rapper americano con claras ideas políticas que llevar adelante, particularmente en sintonía con la visión anárquica o casi libertaria de los Hackers. Jello declara abiertamente su aversión al gobierno Bush, culpable en su opinión de la muerte inútil de tantos miles de jóvenes soldados americanos, de más de veinte mil civiles en Iraq y de la crisis que está atenazando al país. Por ello, tristemente, repite que las cosas no van a cambiar con las próximas elecciones, debido a que también Kerry (el adversario de Bush) está hecho de la misma pasta y en su momento estuvo implicado en las oscuras maniobras de la administración. "Resultaba agradable cuando en América existían dos partidos distintos", ha afirmado explicando cómo a decenas de miles de ciudadanos negros y pobres de Florida se les impidió en su momento el derecho al voto insertándoles de modo fraudulento en una lista de personas que habían perdido ese derecho. (Bush ganó en Florida por unos seis mil votos de diferencia y la población negra y pobre desde luego que no pensaba votar a Bush. La comisión que posteriormente debía analizar lo ocurrido estaba compuesta por antiguos amigos del padre de Bush. En estas circunstancias, resultaba prácticamente imposible que Al Gore conservara alguna esperanza de llegar a la verdad de los hechos, y acabó cediendo y regalando la victoria a Bush Jr.).

Para cerrar el evento, otra conferencia especialmente esperada: Social Engineering con Emmanuel Goldstein, Kevin Mitnick y Cheshire Catalyst, que no se limitaron sólo a contar anécdotas simpáticas y divertidas, prefirieron soltarse el pelo en una increíble sesión de Social Engineering en vivo... Era difícil pedirle más a una conferencia compuesta por tres intensos días.

LINKS PARA PROFUNDIZAR

HOPE: www.the-fifth-hope.org
China: www.freenet-china.org
Capitán Crunch: http://www.webcrunchers.com/crunch/
Steve Wozniak: www.woz.org
Wheels of Zeus: www.woz.com

Crónica de un ATAQUE al





Un lluvioso día de invierno, la habitual e inútil clase de informática. Todos en el laboratorio como buenos chicos. Pero de pronto...

Un día como tantos otros. Nos sentamos delante del PC del aula de informática y de pronto lo miramos con otros ojos. Allí está, parcialmente defendido por una caja cerrada con un candado. Y de pronto, llega una fuerte sensación, una manía de búsqueda, de desafío. Un no sé qué de presunción de cometer una acción criticada por muchos, pero al mismo tiempo demostrar la propia capacidad.

Lo miramos y, en el fondo, ya no es tan inaccesible: existe la posibilidad de insertar CDs y floppies. Ya lo conocemos, lo hamos usado antes: el habitual, y apolillado, Windows 2000 Professional, un antivirus Symantec no desactivable y, lo saben todos, la cuenta Profesor accesible sin password - grupo: users.

Nace el desafío en un rincón de nuestro cerebro. No se puede volver atrás, debemos probar, es una sensación... de excitación inminente.

Insertamos un floppy de boot y un CD de boot en el PC y arrancamos. Si funciona obtendremos un shell de DOS, pero por desgracia el admin ha configurado la BIOS para que siga el siguiente orden:

1) Hard-disk
2) CD-ROM
3) Floppy

Si el admin hubiera olvidado configurar el password de la BIOS no habría problema, pero pulsando SUPR al arrancar hemos visto que estaba configurado y así estamos un poco más alerta. ¡Pero no nos vamos a detener por tan poca cosa!

Nos hemos conectado y hemos tomado un par de informaciones. Olvidamos todo lo que creemos saber sobre pwdump y samdump que deberían extraer la lista de cuentas para trabajarlas luego con lophtcrack: ¡no es cierto! Lo hemos descubierto con la práctica, no funcionan y además hay que ser administrador para poder usarlos, por lo que el único modo de resolverlo es instalar en el equipo lc4 y dejar que lo extraiga él. El problema es que para poder extraerlo necesitaremos pertenecer al grupo administrator. Ahora la pregunta es: ¿Cómo conseguimos convertirnos en administrator?

Convertirse en admin

Primero pensamos usar el programa sechole.exe, que permite ser administrator, pero no funciona en todos los Windows y además, el antivirus activado no permite que se inicie. Reiniciamos Win2000 y pulsamos F8. Lanzamos el modo a prueba de fallos y renombramos C:\programas\symantec como C:\programas\symantec1 para que el próximo inicio no encuentre ya la carpeta con el antivirus. Un

SERVER de la ESCUELA

buen golpe: ya no hay antivirus, pero sechole no funciona.
La cuestión empieza a ser interesante. La única solución es eliminar el password de la BIOS y en Internet hay muchos programas que lo consiguen, como awcrack.exe, pero no funcionan en Windows 2000, por un problema del sistema operativo no se puede interactuar con la BIOS... Timbre, fin de la clase. Frustración momentánea por no haber conseguido aún combinar nada. Pero el coco le da vueltas...

En casa

Es como un loop cerebral, sigue funcionando, aunque no pienses en ello... Así funcionan los procesos mentales. Y de pronto, por sí sola, aparece ¡la solución!
Cuando se inicia el equipo hay una función que se denomina SKIP que se puede reclamar para hacer saltar el reconocimiento del disco duro y del CD-ROM. Así, si este pobre proceso no hubiera visto el disco duro ni el CD-ROM lo habríamos conseguido: ¡podríamos arrancar desde el floppy!

La mañana después

Aquí estamos de nuevo, y lo tenemos. Hacemos el skip y como queríamos demostrar: ¡arranca el floppy! Hemos insertado un floppy de boot de Win95. Obtenido el shell, lo hemos sacado. Insertamos un floppy de nuestro arsenal para emergencias de este tipo... que contiene awcrack.exe y listo, iniciado.
Desde un shell de DOS funciona de maravilla. Reiniciamos, configuramos la BIOS para que pueda ver como primer boot el floppy. Reiniciamos otra vez, vuelve el shell, ponemos otro disquete con:

```
awcrack.exe
ntcp.exe
sysshell.exe
```

Win2000 se basa en una partición NTFS que, claro, la FAT32 del floppy no lee, así que usamos ntcp.exe:

```
ntcp //hda1/winnt/system32/spoolsv.exe //hda1/winnt/system32/spoolsv.old
ntcp sysshell.exe //hda1/winnt/system32/spoolsv.exe
```

Reiniciamos...

Abrimos paréntesis:
Systemshell (sysshell.exe) es un programa que sustituye a spoolsv.exe en el inicio para que aparezca un shell con privilegios de administrator.
//hda1 <—- Primer hard-disk primera partición (es como decir C:)

¡Voilà! ¡Nos hemos conectado como profesor y he aquí nuestro shell!
net localgroup administrators profesor /add

Reiniciamos...

He sacado sysshell.exe
Shell del disquete e:
ntcp //hda1/winnt/system32/spoolsv.old //hda1/winnt/system32/spoolsv.exe

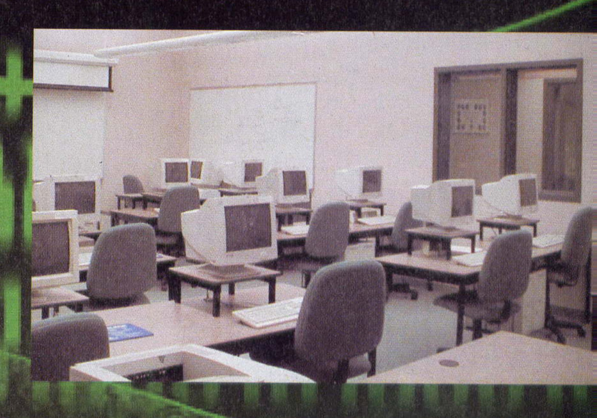
Reiniciamos...

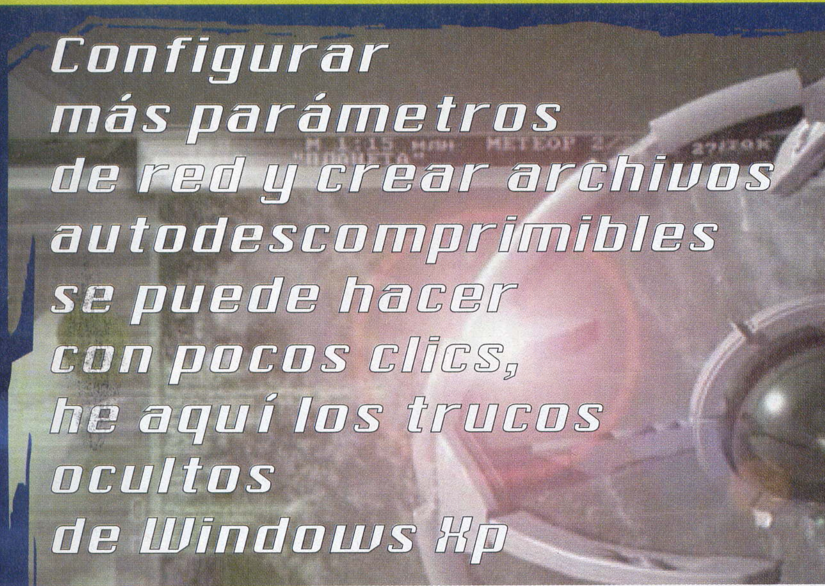
¡Somos admin! Instalamos ya lophtcrack 4.0 y descargamos un diccionario de palabras españolas y el crack para el programa que es de pago (¡pues sí!) Saltamos el password y lo guardamos en un floppy.
"Y por lo tanto el problema de la seguridad de los ordenadores está siempre de actualidad, y los consultores del mundo de la empresa intentan encontrar chicos despiertos como vosotros que han profundizado en el conocimiento y han estudiado a fondo las redes y ordenadores, como tendríais que hacer vosotros, si queréis llegar a conseguir algo en la vida."
Me llegaba de fondo el habitual parloteo del profesor, que a veces era incluso simpático, pero vive en un mundo que parece ajeno... Entretanto, no mira y puedo empezar a romper el password.

Lophtcrack 4.0 en un Athlon 1050mhz y 256ram ddr encuentra:

longitud pass	tiempo
Menos de 7	Max 10 min.
Entre 7 y 13	Max: 6 horas
14	Max 12 horas

¡Listo! Ha resultado ser una mañana muy provechosa.





Configurar más parámetros de red y crear archivos autodescomprimibles se puede hacer con pocos clics, he aquí los trucos ocultos de Windows Xp



REDES Y PORTÁTILES

Cuando llevamos el portátil de viaje, es normal tener que conectarse a redes distintas, con parámetros diferentes. Es un problema: hay que abrir la conexión de red, ir a sus Propiedades y decidir qué parámetros insertar, según la configuración de la red a la que nos conectamos. Un trabajo ímprobo. Que algunos programas resuelven, pero son programas shareware, que suelen emplear mucho tiempo en cargarse y configurar las cosas e incrementan la nuestra larga colección de aplicaciones. Sin embargo, cuando un comando de Windows simplifica enormemente las cosas y no se necesita más, es perfecto para nuestros propósitos.

Vamos a Inicio -> Ejecutar y escribimos cmd. Estamos en la ventana de comandos. En el prompt C:\> escribimos

```
netsh -c interface dump >red1.txt
```

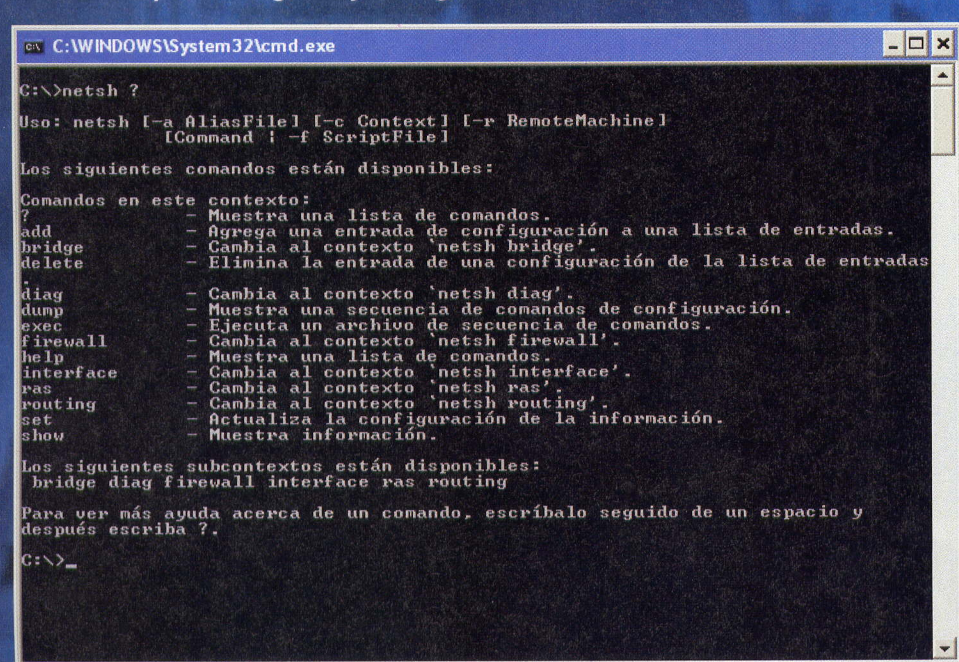
donde en lugar de red1.txt escribimos el nombre de la configuración actual, para recordarla cuando tengamos que usar la misma configuración. Por ejemplo, si estamos en casa, podemos escribir 'Casa.txt', etcétera.

Con esto se crea un archivo de texto (en el directorio en el que se lanza el comando, en nuestro ejemplo C:\), con los parámetros de configuración para la red actual.

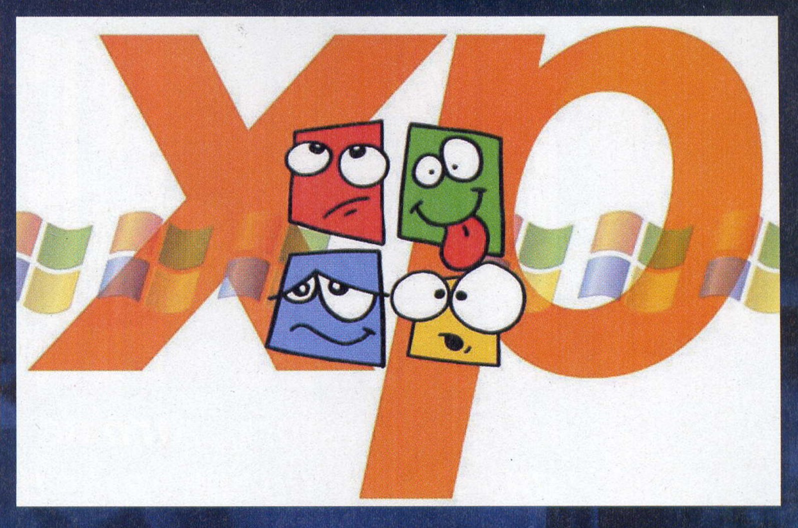
Hacemos lo mismo cuando vamos a la escuela, en casa de un amigo o en otros sitios, creando archivos de texto. Cuando queramos reclamar una configuración, bastará escribir, en la línea de comandos:

```
netsh -f red1.txt
```

donde en lugar de red1.txt escribiremos el nombre del archivo correspondiente al sitio donde nos conectamos.

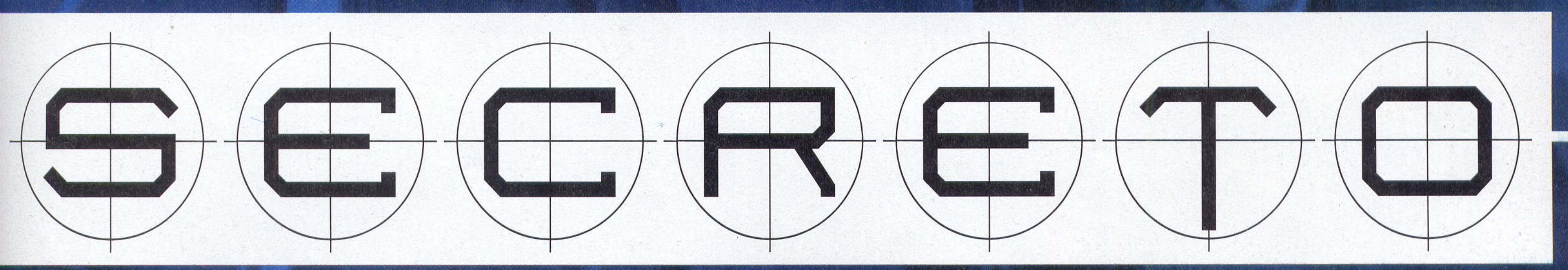


IExpress permite crear archivos autodescomprimibles en pocos clics y sin ningún software complementario



¡MÁS VELOZ!

Durante la fase de compactado de archivos aparece una ventana DOS donde se ejecuta el programa Cabinet Maker. Si hemos insertado archivos grandes o ya comprimidos, el proceso es bastante largo. Maximizar la ventana (con un clic en el cuadrado de pantalla completa arriba a la derecha) lo acelera notablemente.



EMPAQUETAR ARCHIVOS

Este truco ha sido indicado por un lector y utiliza una herramienta de Windows oculta y poco conocida, que permite empaquetar diversos archivos en un único .exe autodescomprimible, creando un verdadero sistema de distribución de archivos, con todas las posibilidades de insertar términos de licencia y ganar espacio por la compresión. Usa un wizard que sigue todas las fases de creación del paquete, y se invoca desde Inicio escribiendo:

```
iexpress
```

Aparece una ventana donde se indica si vamos crear un archivo autodescomprimible o a descomprimir uno.



Ahora especificamos si el archivo que vamos a crear será autodescomprimible y lanzar una instalación, o bien si sólo deberá descomprimir los archivos que incluye, o si sólo será un archivo comprimido, sin opciones de descompresión automática.

IExpress Wizard

Package purpose

Select final result of the package.

- Extract files and run an installation command
- Extract files only
- Create compressed files only (ActiveX Installs)

Description: Files will be expanded to a temporary folder. The files will then be used by the specified installation program.

< Atrás | Siguiente > | Cancelar

En la tercera ventana debemos dar un nombre al paquete, y en la cuarta podemos insertar un mensaje que aparecerá al usuario final y pedirá confirmación antes de descomprimirse automáticamente.

Ahora podemos insertar la llamada a un archivo de texto con una licencia de uso, o un texto de ayuda o cualquier otra cosa. Finalmente, con el botón Add, agregamos los archivos que queramos empaquetar.

IExpress Wizard

Confirmation prompt

- No prompt.
- Prompt user with:

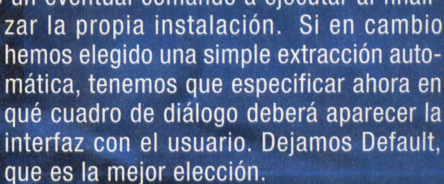
¿Preparado? ¡Vamos a descomprimir!

< Atrás | Siguiente > | Cancelar

Si hemos elegido lanzar un programa de instalación, ahora se nos pide que especifiquemos el nombre y podemos escribir incluso un eventual comando a ejecutar al finalizar la propia instalación. Si en cambio hemos elegido una simple extracción automática, tenemos que especificar ahora en qué cuadro de diálogo deberá aparecer la interfaz con el usuario. Dejamos Default, que es la mejor elección.





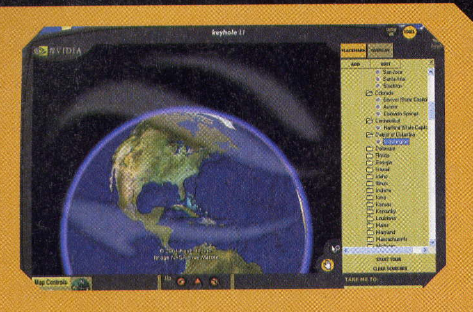
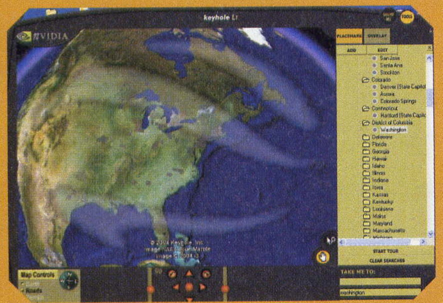
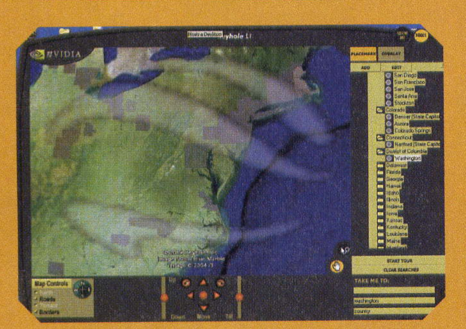


Especificamos un eventual mensaje de salida y finalmente damos una ruta y un nombre al archivo resultante. Podemos guardar todos los parámetros indicados para una próxima ocasión, y finalmente creamos el paquete: aparece una ventana con algunas estadísticas.





Si el archivo no es muy grande, lo que ganamos en compresión lo perdemos en instrucciones para la descompresión. Otro inconveniente es que, a diferencia de un archivo .zip, al enviar un .exe será bloqueado inmediatamente por todas las protecciones antivirus.




GRAN HERMANO

El Pentágono: centro de la defensa americana, uno de los lugares más blindados del planeta. Vamos a descubrirlo con un programa que hará de nuestra búsqueda de ingeniería social una experiencia espacial

Ante todo necesitamos un programa especial, que se distribuye libremente y que, en teoría, dura sólo siete días. Lo encontraremos en la dirección http://www.keyhole.com /downloads/KeyholeLT172r3.exe. Tras el registro, abierta la ventana principal, usamos los cursores abajo en el centro para movernos o bien el botón secundario del mouse sobre la vista para subir, bajar y situarse por todo el globo.

A la derecha, indicamos bajo el botón Tools -> Placemark -> North America -> United States -> District Of Columbia la ciudad de Washington. Doble clic sobre el nombre y en la ventana principal empezará el guiado automático.

Apenas llegar a Washington, tenemos que hallar el Pentágono. No hemos estado nunca, pero como todas las grandes ciudades del mundo Washington tiene metro y es imposible que no exista una parada específica para un sitio donde trabajan miles de personas. Para ver las líneas de metro activamos la función Show Me -> Subway Lines, en la zona izquierda de la imagen del programa. Entre paréntesis, ya que estamos: ¡podemos ver por fin las pizzerías, funcionando en Washington!



Un clic secundario sobre la "i" y vamos directamente al foro de usuarios

¡Localizado! Una parada en el cruce de la línea azul con la amarilla se llama precisamente Pentagon. Nos acercamos, usando el botón secundario y moviendo el mouse. Llegamos a una definición de imagen espectacular, que alcanza a ver hasta detalles de casi un metro. Con el cursor Tilt nos situamos para ver el edificio en perspectiva.

Activamos la tecla Keyhole Community BBS, justo sobre la que ha mostrado las líneas de metro. en el centro del Pentágono aparece una "i" sobre fondo azul: indica que podemos intercambiar con otros usuarios información sobre el lugar. Un clic sobre la




GALÁCTICO

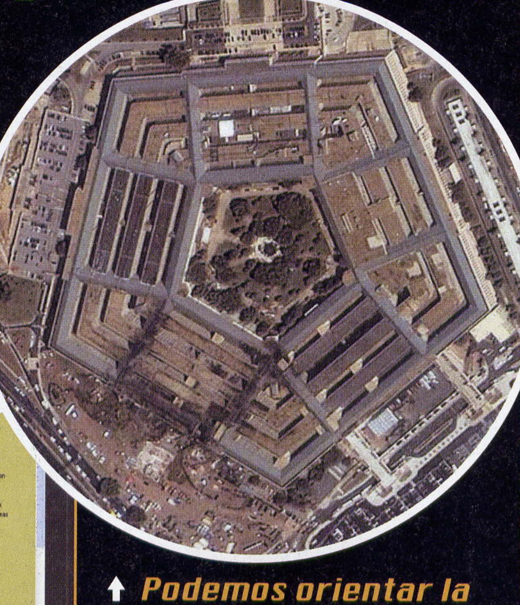


SE REQUIERE UNA CONEXIÓN VELOZ

Esta es la ocasión ideal para convencer a los padres para contratar ADSL: ¡no han visto nunca búsquedas de geografía a este nivel!
Si intentamos la conexión de Keyhole con un módem a 56 K podemos quedar frustrados para toda la vida...: no vale la pena, aunque siempre puedes probarlo si eres de los que no se desaniman fácilmente.

"i" del mappa con el botón secundario y vamos directamente al foro de usurarios, en el thread que habla del Pentágono. Un participante sugiere ir a visitar el Pentágono por dentro, mediante una visita guiada virtual, en la dirección http://www.defenselink.mil/pubs/pentagon/fullvideo56.ram Lo haremos, pero antes queremos ver la foto de satélite tras el horrible atentado del 11 de septiembre de 2001. Un salto a la dirección http://www.spaceimaging. com/gallery/9-11/default.htm# permite ver una imagen de satélite con lo que estamos viendo mediante Keyhole. Impresionante, podemos girar la imagen de Keyhole para ver exactamente la misma orientación y el mismo tamaño de la imagen estática tomada por el satélite.

Puedes visitar cualquier otro sitio, como tu ciudad, tu propia casa... o bien otras áreas misteriosas y fascinantes, como el Área 51, o las más pequeñas islas en medio del océano atlántico, en algunos casos convertidas en depósitos de escoria radioactiva. ¡Tenemos todo el mundo a nuestro alcance!

↑ *Podemos orientar la vista del Pentágono en Keyhole para confrontarla con una foto tomada el 11 de septiembre de 2001*





TERRORISTAS



Usaban el teléfono móvil con tarjeta de Suiza, pero la tecnología les enganchó. ¡Una lección ejemplar!

La operación Mont Blanc empezó casi por casualidad en abril de 2002, cuando las autoridades suizas interceptaron una llamada de menos de un minuto, totalmente silenciosa. El 11 de septiembre era aún muy reciente y los investigadores se preguntaron si aquella llamada podía ser una señal convenida entre terroristas. Lo era. La operación duró casi dos años y llevó a descubrir y desmantelar células del terror en tres continentes. Con un único denominador: el móvil con tarjeta.

BIN LADEN Y LOS MENSAJES



Durante los bombardeos de Tora Bora en Afghanistan de diciembre de 2001, las autoridades americanas comunicaron que habían oído a Osama bin Laden hablando con sus contactos mediante un teléfono por satélite. Ahora, si aún sigue vivo, prefiere comunicarse mediante cartas convencionales transportadas por correos fieles.

Esto no es seguro, aunque no se haya firmado un contrato. Una de las presuntas mentes del 11 de septiembre, Khalid Shaikh Mohammed, es la víctima más excelente de la operación. Fue arrestado en marzo en Pakistán. Ello se debió en gran parte a las intercepciones telefónicas realizadas sobre móviles de los sospechosos, y a un clamoroso error de cálculo de estos últimos. Habían adquirido numerosas tarjetas de móvil de Swisscom, preferidas

ENGANCHADOS SIEMPRE AL MÓVIL

porque podían comprarse proporcionando un simple nombre, incluso falso, y permitían llamar a todo el mundo. La investigación empezó en Suiza e implicó unos diez países más, incluyendo Italia, Estados unidos, Pakistán, Arabia Saudí, Alemania y Gran Bretaña. La llamada que lo inició todo ocurrió el 11 de abril de 2002, cuando Christian Ganczarski, musulmán polaco treintañero nacido en Alemania y sospechoso de estar vinculado con Al Qaeda, marcó el número de Khalid Shaikh Mohammed, entonces en sitio seguro en su refugio del Pakistán.

La llamada debía avisar a Mohammed de un atentado suicida en una sinagoga tunecina, ocurrido el mismo día y que costó la vida a 21 personas, casi todos turistas alemanes.
Dos semanas después del atentado la policía realizó un registro en casa de Ganczarski y halló una lista de números de móviles, incluyendo el interceptado, que llevaba hasta Mohammed. Posteriores pesquisas llevaron a descubrir las predilecciones de los terroristas por la tarjeta Subscriber Identity Module Cards de Swisscom. ¿El error de Mohammed? Usaba muchos teléfonos, y las autoridades no conseguían aislar su posición, pero usaba siempre la misma tarjeta SIM.

El arresto de Mohammed ha llevó al descubrimiento de un centenar más de números de teléfono, además de ordenadores y muchos móviles. En cadena, los números descubiertos llevaron a controlar más de seis mil contactos telefónicos, diseñando en la práctica un mapa virtual de las comunicaciones de Al Qaeda.

Ahora la operación Mont Blanc ha dado todos los resultados que podía dar y prácticamente ha concluido, aunque las autoridades siguen teniendo bajo control un número limitado de tarjetas. Entretanto, el uno de julio de 2004 entraba en vigor en Suiza una ley que prohíbe la adquisición de tarjetas para móviles a menos que el comprador proporcione un mínimo de datos personales.

La operación Mont Blanc probablemente nos ha aportado más seguridad. Pero ha confirmado que nuestras comunicaciones no lo son tanto.

Para las autoridades encargadas de la lucha contra el terrorismo el SIM Swisscom usado por Al Qaeda no tenía precio.

Todas las imágenes provienen de Global Locate, Inc.

THE BIG GUY



En junio de 2003, entre el centenar de llamadas interceptadas en el transcurso de la operación Mont Blanc, una decía "está llegando el pez gordo. Estará aquí pronto". El pez gordo resultó ser Abdullah Oweis, árabe saudí, puntal de la organización de Al Qaeda, a sus anchas tanto entre los occidentales como entre los mujahiddin. Oweis fue arrestado en Qatar el pasado julio.



Tras el 11 de septiembre la actividad de interceptar llamadas ha crecido sin medida en todo el mundo. Aquí se ve un momento posterior al impacto contra el Pentágono de uno de los aviones desviados.



AL-ZARKAWI Y LAS LLAMADAS EN CLAVE

En 2002 las autoridades alemanas interceptaron varias veces a Abu Musab al-Zarkawi, sospechoso de pertenecer a Al Qaeda, mientras ordenaba ataques terroristas contra objetivos judíos en Alemania. Las intercepciones llevaron a aislar y desarticular una célula terrorista pero todavía no a encerrar a al-Zarkawi, que parece ser que ahora se limita a llamadas brevísimas, compuestas de pocas palabras en clave.

Trucos y secretos sin arriesgar

Ya podemos probar sin miedo el mejor sistema operativo gratuito del mundo. ¡Mejor incluso que Windows, que es de pago!

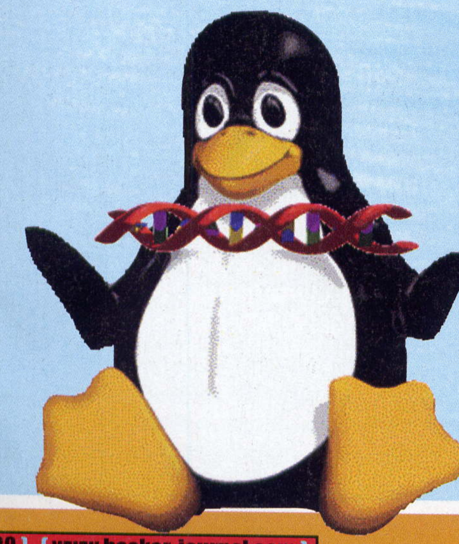
Ante todo tenemos que conseguir una distribución correcta. Desaconsejamos Slackware y Debian por su complicación; una distro [*alias* de distribución] adecuada para todos puede ser Mandrake, de la que se pueden encontrar las imágenes de disco ISO en Internet.

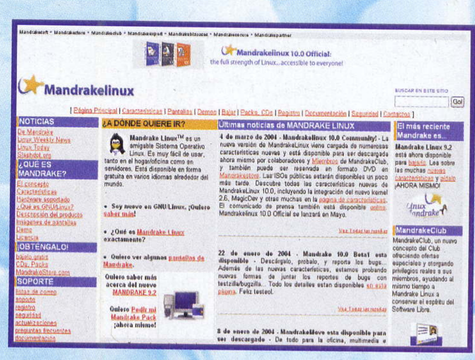
Son 3 CD, v. 9.2 en este momento, disponibles en http://www.mandrakelinux.com/. Comprobamos la compatibilidad de los componentes de hardware con Mandrake, en http:// www.mandrakelinux.com/en/hardware.php3; si no hemos encontrado algún hardware, en Google, escribe "linux" + "nombre_del_ componente_hardware" y pulsa "Voy a tener suerte". Los drivers aparecerán con facilidad.

Cuidado con la grabadora

Si tenemos una grabadora o unidad lectora CD/DVD de la marca LG hay que leer también http://www.mandrakelinux.com/en/lgerrata.php3, porque la mdk [alias de Mandrake] podría sobreescribir el driver, dejando a la unidad fuera de combate.

Una vez descargados los CD de la distro, tenemos que instalarla, con dos opciones: boot desde CD o boot desde floppy. Para el boot desde CD hay que cambiar la BIOS. Cuidado con los errores, que pueden ser graves; es mejor pedir ayuda a alguien experto. Si no queremos cambiar la BIOS,





▲ *En la dirección http://www.mandrakelinux.com/es/ se puede saber todo sobre Mandrake en español.*

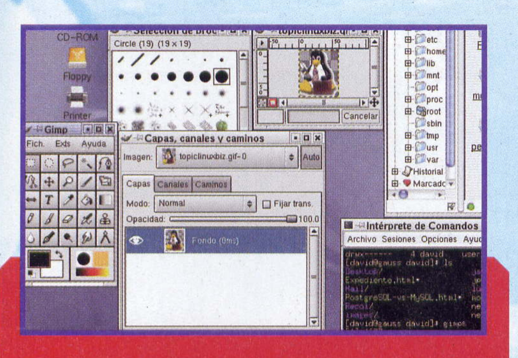
podemos crear una imagen con la utilidad RawWrite presente en dosutils/rawrite.exe del CD 1 de Mandrake, escribiendo en MS-DOS:

```
C:\>cd D:\
D:\>dosutils\rawrite.exe -f images\cdrom.img
```

donde D:\ representa el lector de CD. Hacemos un backup general, un scandisk y un defrag, y reiniciamos el equipo con el floppy/CD insertado. El instalador se inicia automáticamente. Pulsamos Intro cuando se nos indique y esperamos que se cargue el programa. Lo primero que hay que configurar es el idiom. Luego viene la licencia. La leemos y pulsamos sobre "Acepto", y luego "Siguiente". Ahora se configura el mouse: normalmente lo reconoce automáticamente. Si falla, indicamos el nuestro. Hacemos algu-



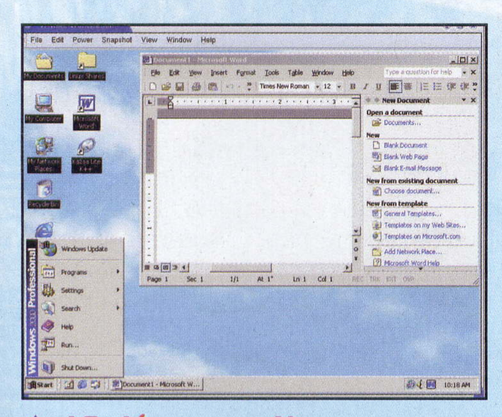
para instalar LINUX Windows



▲ Basta con elegir el idioma: Mandrake se comporta bien con cualquiera.

nas pruebas (pulsando en Siguiente aparece una ventana donde se puede probar el mouse).

En el paso siguiente indicamos el nivel de seguridad. Para un uso personal el nivel "Normal" es suficiente. El particionado, la fase siguiente, es la subdivisión del disco duro en varias partes. Seleccionamos "Usar el espacio libre de la partición de Windows" y pulsamos "Siguiente" para redimensionar la parte de disco duro donde reside Windows. Deja algo de espacio libre, o se producirá una crisis a la menor operación.



▲ ¿Quién necesita usar Windows, si Office puede funcionar perfectamente bajo Linux?

Al pulsar la tecla "Siguiente" encontramos la indicación de los puntos de montaje (o sea, en qué particiones se instalarán las carpetas "/" y "/home"); pulsamos "Siguiente" porque la configuración estándar ya va bien. Tras el formato de las particiones, instalamos el software y, al finalizar, empezamos a configurar el sistema.

root, el usuario divino (para bien y para mal)

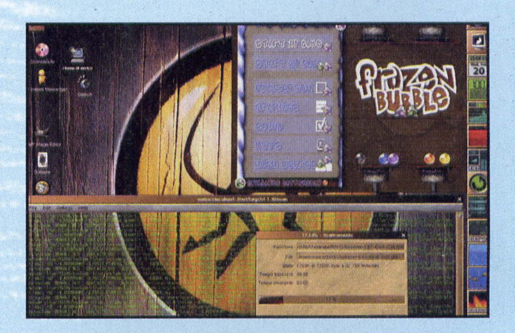
Hay que especificar el password de root, el usuario con control total del sistema. No conviene trabajar normalmente como root, porque un error usando este usuario puede ser irreparable (si escribes como root el comando tee en /etc/fstab tendrás que reinstalarlo todo...); indicamos el password y lo guardamos en lugar seguro.

Ahora se crea un nuevo usuario, del que hay que indicar el nombre y el password, más el nombre real y el icono. Este usuario es el que usará diariamente; usaremos root sólo en casos especiales, como la instalación



▲ La autopresentación de Mandrake!

de software (como user normal no tienes el permiso de escritura en /usr y otras carpetas del sistema). Luego hay que elegir qué bootloader instalar, es decir, el programa que permite decidir qué sistema operativo iniciar al arrancar el equipo; finalmente, nos encontraremos ante una ventana de resumen. Se nos preguntará si queremos buscar actualizaciones de software por Internet: elegimos y seguimos adelante. El sistema se reiniciará y, en adelante, podremos elegir el SO que queremos iniciar. A divertirse con Linux ;-)



▲ ¡No faltan ni siquiera los juegos!

ARTE DEL CÓDIGO

¡Os vamos a contar

La criptografía es el arte de elaborar algoritmos para cifrar un mensaje y hacerlo incomprensible para todos excepto el destinatario.

En este artículo explicaremos las diversas posibilidades de cifrado de nuestros archivos: los algoritmos de clave pública, los de clave privada, las funciones de Hash y PGP.

Los algoritmos de clave pública

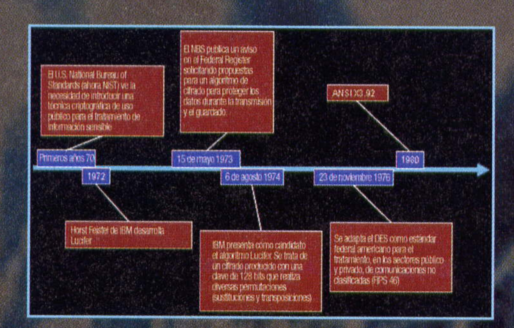
Si un documento se cifre con clave pública, ni el emisor ni el destinatario conocen la misma clave (uno de los principales problemas de la criptografía no es hacer ilegibles los mensajes, sino comunicar de modo seguro la clave de decodificación). Emisor y destinatario usan una copia de claves cada uno: una pública y una privada. Cuanto más larga es la clave, más difícil resulta de adivinar; con un algoritmo simétrico con clave de 80 bits el atacante, a base de fuerza bruta, tiene que probar como máximo 2^80 claves antes de encontrar la clave correcta. En cambio, con un algoritmo de clave pública de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits, con hasta 155 cifras decimales.

El trabajo del atacante es muy distinto según el algoritmo utilizado. Los algoritmos más importantes de clave pública son RSA, ELGAMAL, LUC y Cifrado de probabilidades.

. RSA

Lo desarrollaron en 1977 Ron Rivest, Adi Shamir y Leonard Adleman. Se basa en el análisis de la factorización. Sólo es comparable a otros algoritmos de clave privada como DES, que es mucho más veloz.

RSA proporciona tamaños de clave sólo hasta 2.048 bits.



El inicio de la criptografía moderna y la aparición de DES.

. ELGAMAL

Se basa en el análisis de logaritmos discretos. en estudios recientes se ha evidenciado que RSA y ELGAMAL ofrecen una seguridad parecida por claves diferentes. Pero ELGAMAL es más lento respecto a RSA.

. LUC

Desarrollado por un grupo de investigadores australianos y neozelandeses en base a la secuencia de Lucas, parecida a la más simple de Fibonacci, en la que cada número se obtiene de una operación sobre los números anteriores (como 1, 1, 2, 3, 5, 8, 13, 21... donde cada número es la suma de los dos números anteriores).

. Cifrado Probabilístico

Otra aproximación distinta al cifrado creado por Goldwasser y Micali, que confunde a un interceptor no deseado originando más texto cifrado que el que había en el mensaje de origen.

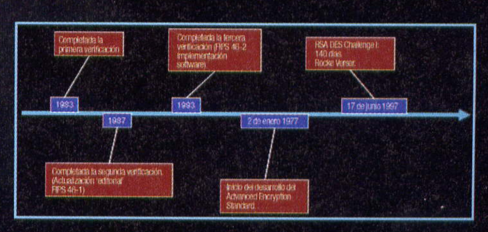
Los algoritmos de clave privada

Los algoritmos de clave privada se diferencian de los de clave pública porque el emisor y el destinatario deben conocer la misma clave secreta. Existen diversos sistemas, incluyendo DES (y sus variantes), IDEA, RC5 y BLOWFISH.

. DES

El algoritmo DES (Data Encryption Standard) nació por exigencia de la NSA (National Security Agency) quien, hace unos 35 años, convocó un concurso para obtener un algoritmo de cifrado avanzado.

Ganaron los técnicos de IBM y, desde 1977 hasta ahora, DES ha sido uno de



En junio de 1997 se violó por primera vez el código DES. Representó la caída de un mito, según la antigua tradición.

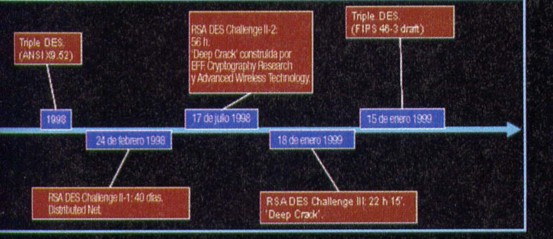



EL ABC DE LA CRIPTOGRAFÍA!

SECRETO

los mejores sistemas para el cifrado de datos (sólo recientemente se han descubierto sus debilidades).

DES pertenece a la familia de los algoritmos simétricos y funciona sustituyendo y desplazando caracteres. El bloque de datos que elabora cada vez es de 64 bits, o sea 8 bytes. También la clave es de 64 bits, pero sólo se utilizan 56 de ellos. Los demás bits se utilizan para el control de paridad. para mejorar DES nació el algoritmo 3DES (Triple DES), que reutiliza DES cifrando tres veces consecutivas el mensaje con diversas claves. 3DES usa tres claves de 56 bits, con un total de 162 de clave. 3DES es claramente más lento que DES y, aunque está más protegido contra un ataque de fuerza bruta, no ofrece la seguridad de otros algoritmos de claves más largas.



↑ *Triple DES consiste prácticamente en aplciar tres veces DES al mensaje. Más robusto que antes, pero la criptografía fuerte es otra cosa.*

. IDEA

Fue ideado en 1990 en el Politécnico ETH de Zurich por James L. Massey y Xuejia Lai. Usa claves de 128 bits y el mismo algoritmo se ocupa de cifrar y descifrar. Está bajo patente hasta el 2007.

. BLOWFISH

Fue inventado en 1993 por Bruce Schneier y propuesto como sustituto de DES e IDEA, y está libre de patentes. Funciona con claves variables de 32 bits hasta 448 bits.

. RC5

RC5 es un cifrado de bloques simple y veloz, proyectado por Ronald Rivest en 1995, en el Laboratory of Computer Science del MIT.
El algoritmo se puede implementar por hardware o por software y se basa en la longitud de las palabras, el número de iteraciones y la longitud de la clave privada.

Funciones HASH

Las funciones hash o one-way hash trasforman un documento de una longitud arbitraria en un código de una lungitud fija. La cadena resultante se define como valor de hash o checksum.
La característica de estas funciones es su dificultad para invertirlas: dado un valor de hash es muy difícil conseguir llegar al mensaje que lo ha generado; por otra parte, es muy difícil producir un mensaje que proporcione un valor de hash predeterminado. La longitud de los valores de hash varía según los algoritmos. Actualmente se utilizan especialmente los siguientes algoritmos: MD2, MD4, MD5, SHA y SHA-1.

MD2, MD4 y MD5

Fueron desarrollados por Rivest en 1990; trabajan tomando un documento de longitud arbitraria y creando un resumen del documento en clave de 128 bits. Se puede encontrar más información en las RFC 1319-1321 (http://www.faqs.org/rfcs/rfc1319.html, 1320.html y 1321.html).

SHA-1

El software de file sharing Bit Torrent utiliza este algoritmo para verificar los archivos. SHA significa Secure Hash Algorithm. Fue desarrollado por investigadores del NIST como se especifica en el SHS (Secure Hash Standard) y forma parte del proyecto Capstone. Toma un documento (cuya longitud debe ser inferior a 2^64 bits) y produce una clave de 160 bits.

PGP

PGP es el acrónimo de Pretty Good Privacy, un programa escrito por Philip Zimmermann. La peculiaridad de este programa es la posibilidad de producir claves robustas con algoritmos de clave pública y privada. Usa RSA para codificar una clave secreta que se usa a su vez para cifrar el mensaje.
PGP es freeware se puede encontrar en http://www.pgpi.org/.

AUTOPSIA

Microsoft qjuiere que la Xbox sea una consola cerrada. ¡PUES NO!



Lo más difícil que hay que hacer para modificar el interior de una Xbox es... abrirla. He aquí cómo se hace. Siguiendo estas instrucciones, se llega a desmontar completamente una Xbox.



Primero: quitamos los topes de goma y los adhesivos.

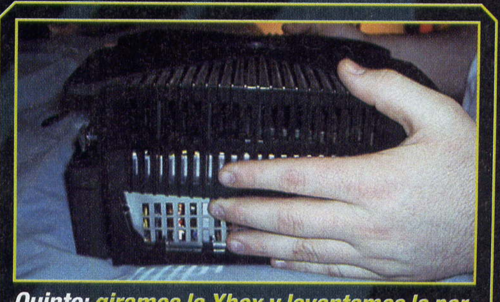


Segundo: Desatornillamos los tornillos bajo las gomas. Usa un destornillador Torx 20.



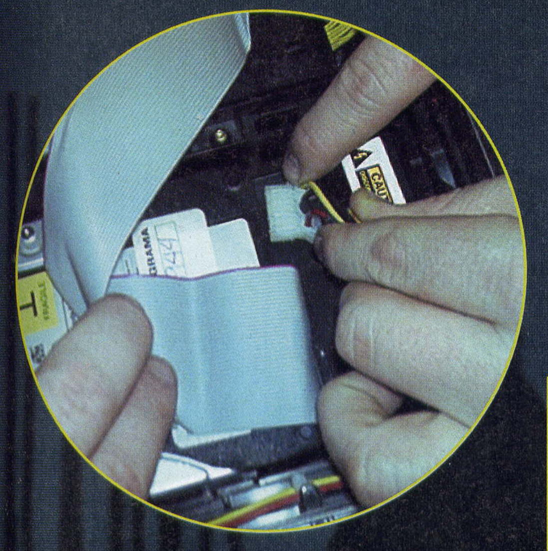
Tercero: desatornillamos el tornillo que está bajo el adhesivo blanco con el código de barras.

Cuarto: desatornillamos el tornillo situado bajo el adhesivo, llamémosle de presentación. Usa el destornillador Torx 20.

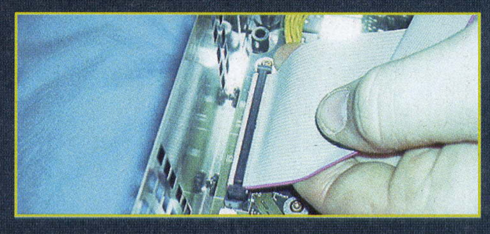


Quinto: giramos la Xbox y levantamos la parte superior de la carcasa.

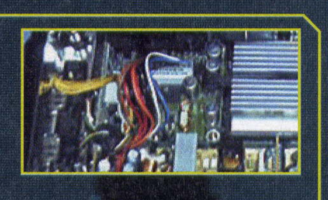
de una XBOX



Sexto: quitamos la corriente al disco duro desconectando el conector de alimentación.

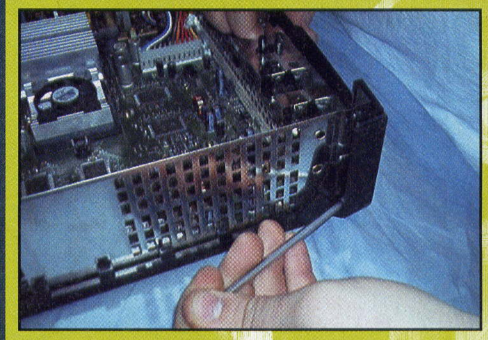


Noveno: separamos el conector IDE de la placa madre.

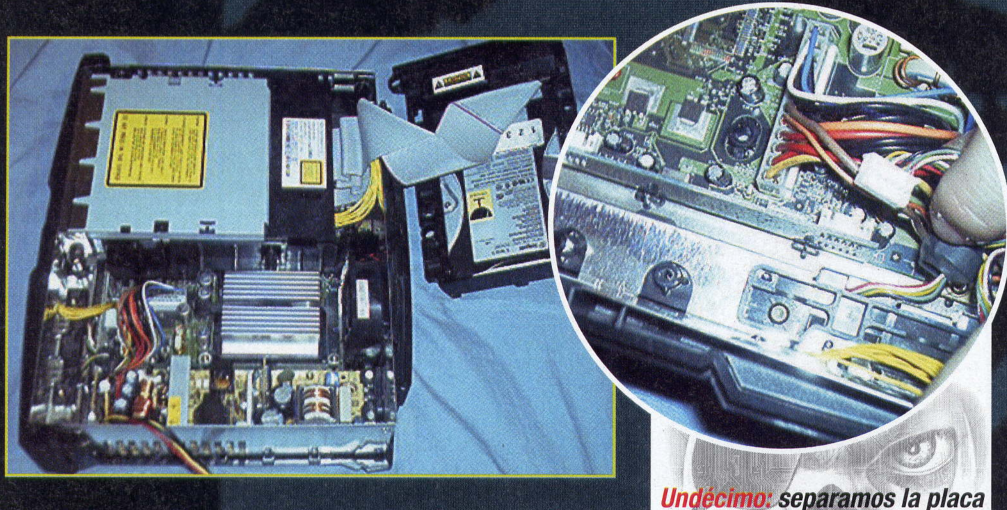


Décimo: desconectamos el conector on/off de la placa madre. Debe estar compuesto de más conectores amarillos, cerca del frontal de la Xbox.



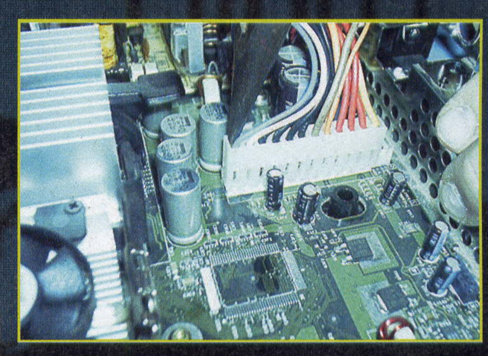


Decimotercero: quitamos el frontal. Hay dos clips frontales y tres clips internos, en el chasis metálico.

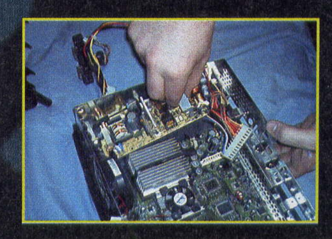


Séptimo: quitamos los tornillos que fijan el disco duro a la consola y leberamos la estructura (chasis más disco duro). Usa el destornillador Torx 10.

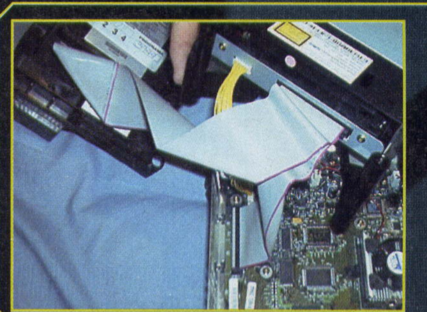
Undécimo: separamos la placa que controla las puertas.



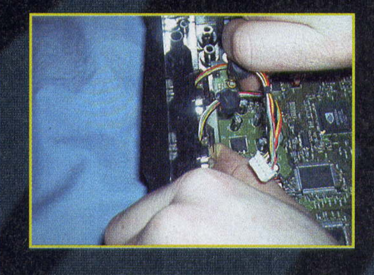
Decimocuarto: separamos el conector de alimentación de la placa madre.



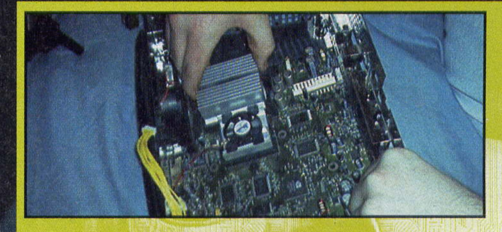
Decimoquinto: sacamos dos tornillos y extraemos la fuente de alimentación.



Octavo: repetimos exactamente la misma operación con el chasis de lector de CD, y quitamos los conectores traseros antes de separar también éste.



Duodécimo: quitamos cuatro tornillos Torx 10 y desmontamos la puerta del controller.



Decimosexto: quedan once tornillos en el camino, pero una vez sacados sale también la placa madre.

MARAVILLAS

Hagamos fácilmente algunos scripts mágicos para la administración de imágenes dentro de una página web

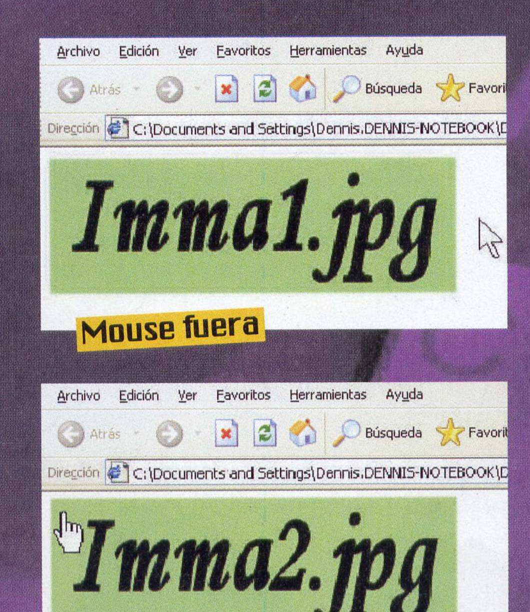


Con Javascript se pueden hacer maravillas, ¿lo sabías? Veamos algunas muy interesantes y útiles para mejorar nuestras páginas.

Los rollover

Los rollover son efectos que podemos crear cuando pasamos con el mouse sobre una imagen (evento onMouseOver) y cuando salimos de la imagen (onMouseOut). Se usan mucho cuando una imagen representa en realidad un link. Un ejemplo:

```
<img src="imma1.jpg" style="cursor:
pointer" onMouseOver="this.src=
'imma2.jpg'" onMouseOut="this.src=
'imma1.jpg'" />
```



Al pasar el mouse por la imagen "ima1.jpg" se cambia por "ima2.jpg". Al salir el mouse, todo vuelve a quedar como al principio. Por otra parte, se establece un css (style="..."), de modo que el cursor cambie y se convierta en una mano.

Con la misma técnica podemos actuar también sobre campos de tipo imagen (<input type="image">).

Otro tipo de rollover puede ser el que modifica el tamaño de una imagen:

```
<img src="imma1.jpg" style=
"height:100px;width:100px;cursor:p
ointer" onMouseOver=
"this.style.height='120px';this.style.
width='120px'" onMouseOut=
"this.style.height='100px';this.style.
width='100px'" />
```



de JavaScript

Efectuar el submit del form mediante una imagen

Para efectuar el submit (el envío) de un form podemos utilizar un botón de tipo imagen, o bien una imagen propiamente dicha.
Basta con cambiar:

```
<input type="submit">
```

Por:

```
<input type="image" src="imma1.jpg">
```

No es una imagen propiamente dicha, sino un input de tipo 'image', de hecho. En el caso en que queramos efectuar el submit de un form a través de una imagen propiamente dicha, actuamos sobre el evento onClick de la misma imagen:

```
<img src="imma1.jpg" onClick="document.NOMBREFORM.submit()" style="cursor:pointer;" />
```

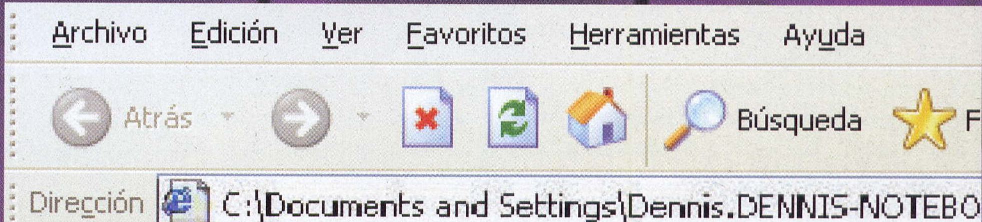
obviamente, NOMBREFORM debe sustituirse por la propiedad name del form que vamos a enviar.

Sustituir una imagen presente por otra

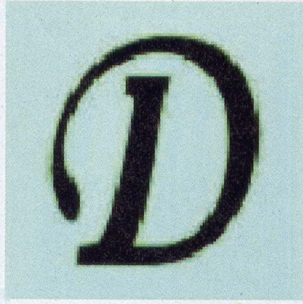
Si tenemos que sustituir una imagen por otra, el método a seguir es crear una función que redefina la propiedad src de la imagen dada:

```
<script>
function cambia_imagen
(cual,nueva){
document.images[cual].src=
nueva
}
</script>

<img name="imagen1"
src="imma1.jpg" />
<input type="button"
onClick="cambia_imagen('imagen1','imma2.jpg')"
value="cambia imagen">
```







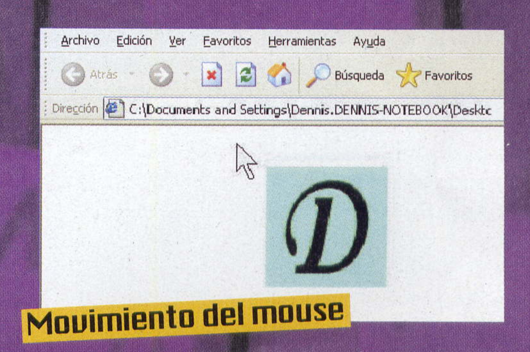
Cargando la página

En este ejemplo hemos creado una función, llamada al pulsar sobre el botón. Si se requiere cambiar una sola imagen, se puede hacer tranquilamente como hemos visto con los rollover, o bien actuar directamente dentro del tag input:

```
<input type="button"
onClick="document.images['imagen1'].src='segunda.jpg'"
value="cambia imagen">
```

Imágenes que siguen al mouse

Se llaman mouse trailers, son imágenes (o iconos), que siguen al mou-



Movimiento del mouse

se por toda el área de la página. En Internet existen muchísimas, si hacemos una búsqueda en un motor de búsquedas cualquier o bien en una colección de scripts encontraremos a mansalva.
para crear una simple, basta con lo siguiente:

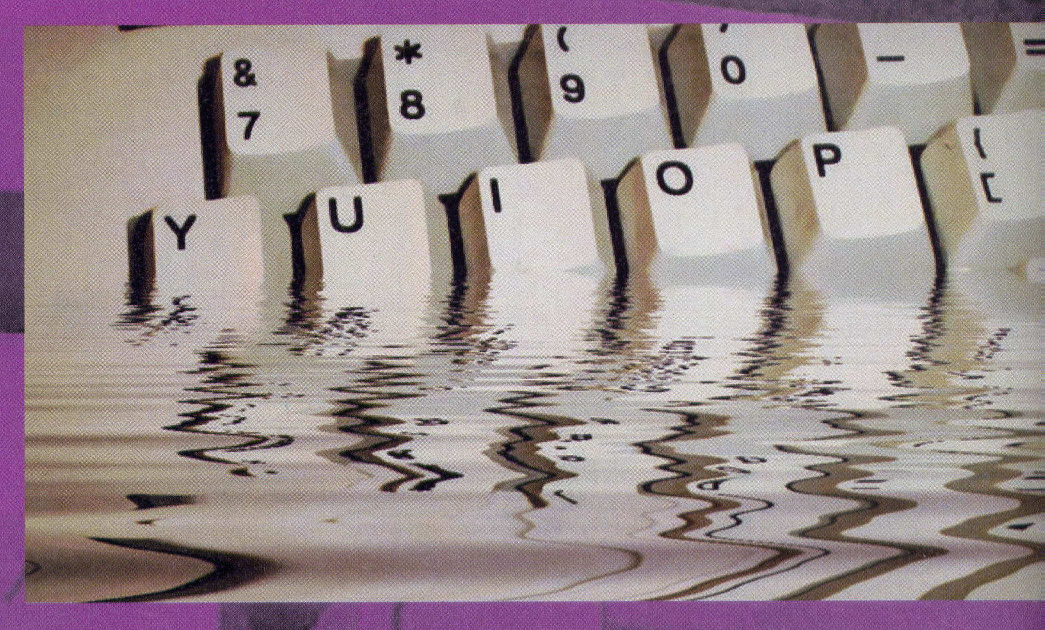
```
<script>
function sigue(){
document.trailer.style.position="absolute"
document.trailer.style.top=event.clientY+15
document.trailer.style.left=event.clientX+15
}
</script>

<body onMouseMove="sigue()">
<img name="trailer" src="imma1.jpg" style="width:100px;height:100px" />
```

debido a que se actúa sobre la propiedad top y left, el posicionamiento de la imagen se configura en el script siendo necesario indicar el parámetro "absolute".
En la función, se configuran top (distancia al borde superior de la página) y left (distancia al borde izquierdo de la página) con las posiciones del mouse, añadiendo 15 píxels a las dos, de modo que la imagen queda un poco desplazada respecto al puntero del mouse.

Imágenes que siguen el scroll de la página

Es posible utilizar un script de este tipo para hacer correr una imagen (pero de hecho sirve para cualquier otro elemento), siguiendo el scroll del navegador.
Lo que hay que hacer en el script es simplemente configurar las dos variables margenX y margenY, los márgenes que la imagen mantendrá respectivamente desde el borde izquierdo y desde el borde superior de la página.

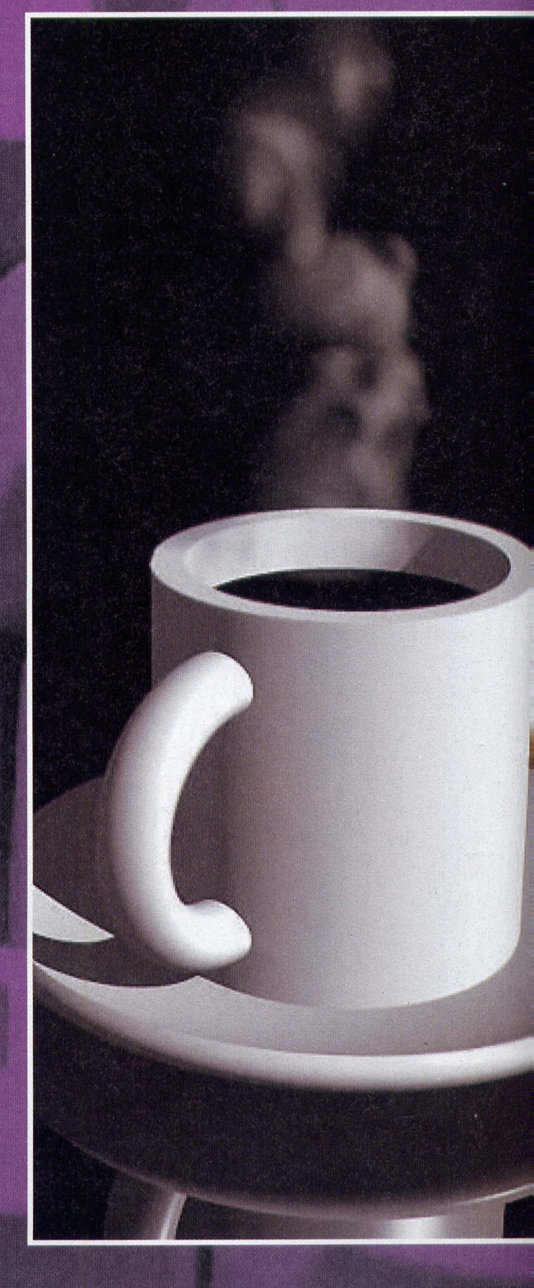



```
<script>
function mover(nombre){
margenX=15;
margenY=30;
ejeY=0;
ejeX=0;
if(document.documentElement && document.documentElement.scrollTop){
  ejeY=document.documentElement.scrollTop;
  ejeX=document.documentElement.scrollLeft;
}
else if(document.body){
  ejeY=document.body.scrollTop
  ejeX=document.body.scrollLeft
}
document.images[nombre].style.position="absolute";
document.images[nombre].style.left=asseX+margenX;
document.images[nombre].style.top=ejeY+margenY;
}
</script>
```

este script será llamado simplemente en el evento onScroll del body:

```
<body onScroll="mover('NOMBREIMAGEN')">
```

El código resulta ser tal vez un poco más elaborado que en los ejemplos anteriores, pero el funcionamiento sigue siendo simple.
Debido a que la función es llamada cuando se produce el scroll (o sea, cuando se desliza la página), redefinimos cada vez la posición de la imagen, y tomamos los valores del scroll pasado añadiendo los márgenes fijados en el script. Por desgracia, el efecto funciona sólo en Internet Explorer y Mozilla (1.0 o superior).
Con script adecuados podemos tener imágenes temporizadas, imágenes random, preload de imágenes y otras operaciones con y sobre las imágenes. ¡Es todo un mundo!



OLORES VIA WEB

El olor del amor, un perfume de flores abriéndose al primer rayo de sol. Un modo nuevo de decirte te amo... ¡¿o la peor de las invenciones posibles?!

Descargamos música, películas, videoclips, mp3, programas, fotos y quién sabe qué más. ¿Pero hemos pensado alguna vez en los olores? Esto es lo que hace el sistema experimentado por Telewest Broadband, una gran empresa inglesa de conectividad. Es como si aquí Telefónica anunciara un dispositivo que, conectado por USB al PC, en lugar de imprimir la foto recibida por Internet de la chica lejana, hace sentir el perfume de su piel. ¿No está mal, verdad? Imaginemos la conversación para encontrar la media naranja. ¿Cómo es tu carácter? ¿Qué te gusta? Y de palabra es fácil decir que estamos hechos el uno para la otra, que el próximo encuentro no virtual será lo más excitante que existe en el mundo, pero... ¿y si luego huele mal? Pero ahora, he aquí en directo el olor de nuestro sueño, el perfume de nuestros deseos. Hasta los más perversos, si es lo que se busca. La peste de la cosa más asquerosa que te venga a la cabeza, para enviar al amigo, es un decir, que te ha quitado la novia.

El sistema funciona con conexiones de banda ancha y no nos preguntéis por qué, pero en las especificaciones, se mezclan oportunamente minúsculas gotas de líquidos adecuados y luego se disfruta de una fragancia especial: el spray resultante podría tener, en nuestra imaginación, efectos realmente increíbles. Y no hablamos, desde luego, del perfume de pastel de miel de la abuela, que sin embargo podría ser un buen regalo para el próximo cumpleaños de mamá...

Anti stress

Fin del stress: nos situamos ante el PC y programamos el invento. ¿Cómo ha ido el día? Puntuamos nuestro stress, de 0 a 10. Con 6, el perfume di granada unido a una pizca de violeta será el antídoto adecuado para relajarse. Si llegamos a 10, un más decidido tabaco mezclado con una docena más de esencias parecidas nos dará una calma que ni siquiera podemos imaginar.

¿Y qué decir de cuando estamos tirados en el sofá, escuchando el mejor Jazz y oliendo los cigarros y el tabaco que se difunde por la habitación, como en los más pestilentes music-pub que hemos frecuentado en New Orleans?

Realismo puro, en una cajita roja con veinte esencias para un total de sesenta deseos distintos. Pero justo depués de la comercialización de la versión Lite, podremos actualizarnos a dos mil olores distintos. ¿El precio? 250 euros por hardware y software, 25 euros al mes para la conexión a la banda ancha.

Es el invento del año, si no termina como el truco del almendruco, como hace ocho años, cuando apareció en Internet una actualización de tags HTML mediante la que hacían creer (?) que era posible enviar olores vía Web.

↑ He aquí la genialidad: interfaz USB, conexión de banda ancha. ¿Precio de las cargas? No se ha divulgado, pero esto pasa siempre... ¿Más información? http://www.telewest.co.uk



Programando COMO ARTISTAS

El código "ofuscado" lo escriben los genios, pero divierten a todos

Obfuscated code, o código ofuscado: es el arte de escribir programas que disponen del código para mostrar un dibujo. ¡Y el código debe funcionar! Mejor aún si el algoritmo está oculto dentro del código, y es difícil de aislar. Escribir código "ofuscado" no está al alcance de todo el mundo. Pero cualquiera puede intentarlo. Quien quiera experimentar, que nos escriba: ¡lo publicaremos! Entretanto, he aquí una galería de algunas pequeñas joyas de la ofuscación.

```
12345678901234567890 1
2345678901234567890 12
34567890123456789012 3
45678901234567890123 4
56789012345678901234 5
67890123456789012345 6
```

CALCULAR LA RAÍZ

Este programa en lenguaje C (http://www.bme.jhu.edu/~rcheong/) calcula la raiz cuadrada de un entero. Estúdialo, porque es una pista... :-)

```
#include <stdio.h>
int l;int main(int o,char **O,
int I){char c,*D=O[1];if(o>0){
for(l=0;D[l              ];D[l
++]-=10){D    [l++]-=120;D[l]-=
110;while     (!main(0,O,l))D[l]
+=    20;    putchar((D[l]+1032)
/20    )    ;}putchar(10);}else{
c=o+      (D[I]+82)%10-(I>l/2)*
(D[I-l+I]+72)/10-9;D[I]+=I<0?0
:!(o=main(c/10,O,I-1))*((c+999
)%10-(D[I]+92)%10);}return o;}
```

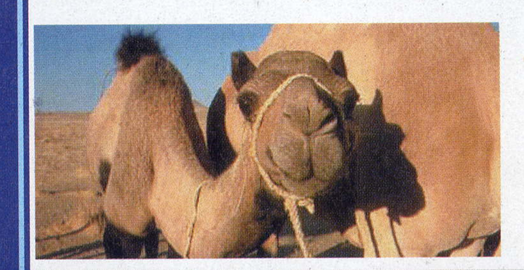
BOLAS, BOLAS, BOLAS

Este programa en Perl (http://www.perlmonks.org/index.pl?node_id=339774) hace en 3D lo que muestra en su forma ASCII:

```
        $_=q%$_="                         88GGCI";
     @a=/./g;@_=('IP                 ""YI','IjjjjI',
    'IiciII')    ;whil              e($c=pop@    a){ma
   p{$_=$c.$_     .$c}@_           ;@_=(($t=(     $n=$a[
  $#a]||"@").$     {c}x(-         2+length$_[0]).$n),@_,
  $t)}$_='j8_4xj4,@@8b,x          j2,@14bxjd@16bxd@18bx@
  20x@20x@20xY@18PxjY@16          Pxj`Y@14Pxj4`@10Pxj8"5
  x';s#(.)(\d*)#$1x($2||          1)#eg;$m=2;$n=-1;$|=1;
   $p=9;$q=20;{$q+=$n*=            $q<11|$q>50?-1:1;$p+
    =$m*=$p<8|$p>16?-1              :1;$u=-$q*6/($l=($
      q**2+$p**2)**.5                 );$v=-2-$p*6/$l;
         $r=$p-6;$                       s=$q-9;$y=0
                          ;select$x
                       ,$x,$x,.2*print
                      "\ec*",(m   ap{$l
                     =0;"\e[".$    r++.";
                    ${s}H",$y++<$v?$_:do{@
                    c=split//,$_[$y-$v-1];
                    map{$l++>$u&/@/&&($t=$
                    c[$l-$u-2])?$t:$_}/./g
                     },$/}splitjx),"\e[30
                      H";redo}%;s#\s##g;
                       s#j#$"#g;eval
```

LA HORA DEL DROMEDARIO

¿Un reloj o una nave del desierto? Hmm. http://perlmonks.thepen.com/190308.htm



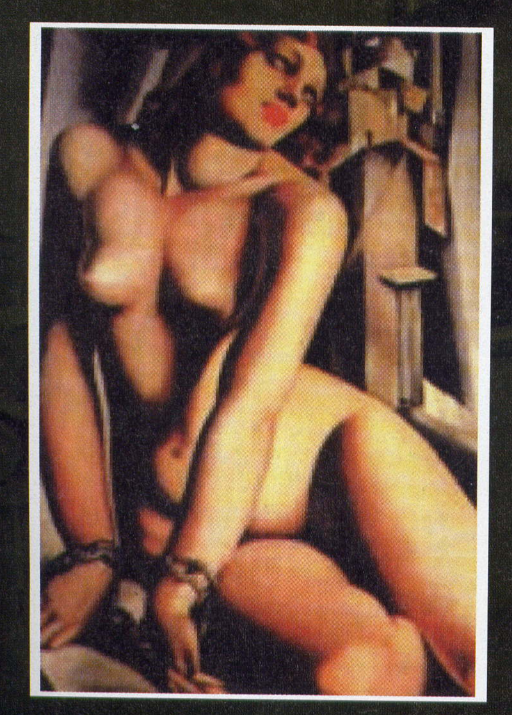
```
#!perl  -w
 use strict;
 $_='
              $,=$/;$|=@_
         =split//,"Justan                       othe
    rPerl.hacker";$/=\'$?~=                (local  tim
  e)[$.]*($.==0||$.==1??1:5);s           ubstr($_,eval
 \\\'$^=$~*2*atan2(1,?1)/15;int(-  cos($^) *($=+
 1)+11.5)*25+int(sin(?$^)*($=+1)+12.5)\\\'?,1,
 $_[$=+(11,4,0)[$.]])?\';do{$_=("."x287).
 "#"."."x287;for$=(0.?.10){$.=0;eval$/;
 $=<7&&($.=1,e                 val$/);$=<4&
  &($.=2,ev                     al$/);}p
    rint(p                        ack("
    c3  ",                         27,9
    1,  72                         ),(/
    .{  25                         }/g)
    ,s  ca                         lar(
    lo   cal                       time)
    );}   whil                     e(slee

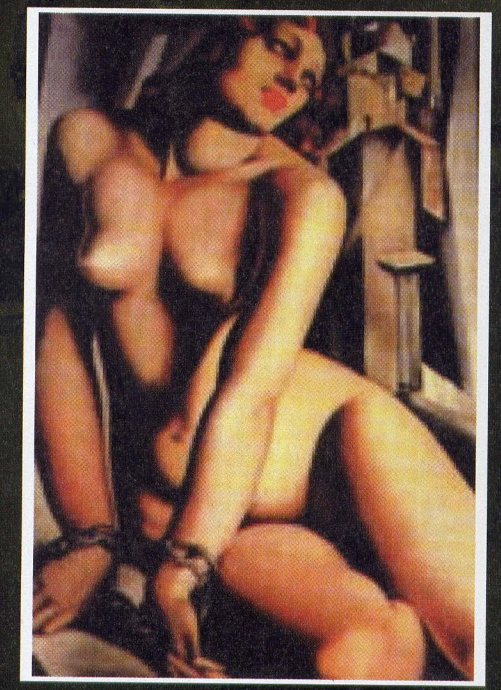
 p(1))';s/\s+//g;eval
```



Contenido Esencial

ESTEGANOGRAFIA





La imagen de la derecha difiere de la de la izquierda porque contiene un mensaje, pero es imposible darse cuenta casualmente

La palabra esteganografía deriva del griego y significa escritura cubierta, oculta. Es el arte de ocultar la existencia de un mensaje, a diferencia de la criptografía, que oculta su contenido. El Web es un campo de aplicación ideal para la esteganografía porque está lleno de información inútil y ruido de fondo, dentro del cual es fácil ocultar un mensaje. Básicamente, esteganografiar es ocultar datos dentro de otros datos que harán invisible su existencia al observador casual. Los datos se ocultarán preferiblemente dentro de archivos gráficos, musicales o bien ejecutables. Como siempre, los únicos programas válidos de esteganografía son aquellos de los que se puede verificar el código fuente.

Gráficos

jphs
http://www.searchlores.org/zipped/jphs_05.zip. Compuesto por JPHIDE.EXE. que oculta los datos en un archivo JPEG, y JPSEEK.EXE, que los recupera.

contraband
http://www.searchlores.org/zipped/contrabd.exe Oculta los datos en una imagen en formato BMP.

Hide and Seek
http://www.searchlores.org/zipped/hdsk41.zip Esteganografía con archivos GIF.

Música

MP3Stego
http://www.searchlores.org/zipped/MP3Stego_1_1_16.zip Oculta los datos en un archivo de música MP3. También se puede utilizar para autenticar un archivo de música, por cuanto el único ataque posible consiste en destruir los datos ocultos mediante descompresión y recompresión del archivo, pero la calidad de la pieza se reduce notablemente.

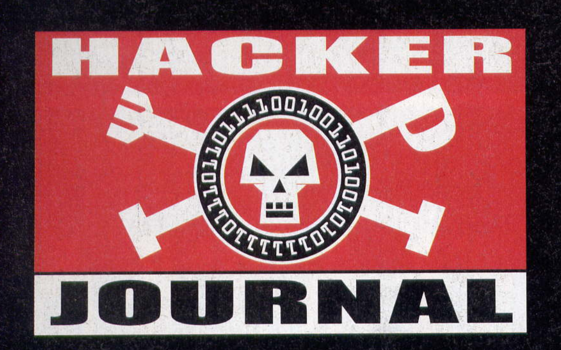
MP3StegoGUI
http://www.searchlores.org/zipped/MP3Stego_GUI.zip. Interfaz gráfica para MP3Stego.

Ejecutables

Hydan
http://www.crazyboy.com/hydan/
El programa utiliza redundancias en el juego de instrucciones de los procesadores i386 y define conjuntos de instrucciones equivalentes desde el punto de vista funcional, para codificar luego la información en código máquina usando las instrucciones apropiadas de cada conjunto. El tamaño del ejecutable queda intacto y el mensaje oculto se cifra con blowfish. Hydan también puede utilizarse para autenticar código.

Espacios en blanco

Snow
http://www.darkside.com.au/snow/
Oculta mensajes en texto ASCII agregando espacios en blanco al final de las líneas. El mensaje puede ir cifrado.



Atrévete con éste...

CYBERENIGMA

Pangrama: frase que se autodescribe en los términos de los caracteres que la componen.

"Esta frase contiene sólo tres veces: a".
Pangrama de nivel 1, realmente facilísimo

"En esta brevísima y clara frase se encuentran siete a y una b".
Pangrama de nivel 2, muy fácil

"Aquí dentro cabe siete veces la a, una vez la b y cinco la c".
Pangrama de nivel 3, fácil

¡El desafío!

Para todos: ¿Qué nivel consigues alcanzar?
Para expertos: Consigue crear un pangrama de nivel 21, con letras del alfabeto español (abcdefghijklmnñopqrstuvwxyz).
Para genios: Consigue crear un pangrama de nivel 26, con todas las letras del alfabeto inglés (abcdefghijklmnopqrstuvwxyz).
Para súper hackers: Consigue escribir un programa para crear pangramas de cualquier nivel.

Las reglas...

La frase es libre.
Los números deben ir siempre escritos en letras (¡si no no es justo!).
Las letras con acento cuentan como vocales normales (á equivale a a, etcétera).

¡Los publicaremos todos!
Escribe a redaccion@hacker-journal.com

www.hacker-journal.com

El muro para tus graffiti digitales